Oracle Key Manager

管理ガイド

バージョン 2.5

パート番号 : E25343-02
2011 年 10 月
リビジョン 01

このドキュメントに関するコメントは STP_FEEDBACK_US@ORACLE.COM に送信してください。

Oracle Key Manager (OKM) 管理ガイド

Part Number E25343-02

Oracle は、このマニュアルを改善するためのコメントや提案を歓迎いたします。STP_FEEDBACK_US@ORACLE.COM にご連絡ください。タイトル、パート番号、発行日、およびリビジョンを含めてください。

目次

図目次

表目次

はじめに

このマニュアルでは、Oracle Key Manager (OKM) ソフトウェアの構成情報および管理情報について説明します。このマニュアルは、使用サイトで OKM ソフトウェアの構成および保守を担当するストレージ管理者、システムプログラマ、およびオペレータを対象にしています。

Key Management System (KMS) という製品名は、Oracle Key Manager (OKM) に名前が変更されています。KMS (そのコンポーネントや概念のほとんど) への参照も、それに応じて変更されています。

Oracle Support へのアクセス

Oracle のお客様は、My Oracle Support を通して電子サポートにアクセスできます。詳細については、http://www.oracle.com/support/contact.html にアクセスするか、または聴覚障害をお持ちの場合は http://www.oracle.com/accessibility/support.html にアクセスしてください。

このリリースの新機能

OKM Release 2.5 には、次の拡張機能が含まれています。

Revision 01

- OKM を Transparent Data Encryption (TDE) とともに構成して、機密性のあるデータベース情報の暗号化または復号化を管理できます。このソリューションでは、Oracle StorageTek テープドライブで使用されているのと同じ暗号化テクノロジーを使用して、Oracle データベースの暗号化鍵を管理できます。

  付録 B、「OKM を Advanced Security の Transparent Data Encryption (TDE) とともに使用する」を参照してください。

- 現在のリリースを反映するために、OKM のスクリーンショットを更新しました。

1

紹介

概要

Oracle Key Manager (OKM) は、暗号化鍵を作成、格納、および管理します。KMS は、次のコンポーネントで構成されています。

- **Key Management Appliance (KMA)** − ポリシーベースのライフサイクル鍵管理、認証、アクセス制御、および鍵プロビジョニングの各サービスを提供する、セキュリティーが強化されたボックスです。ストレージネットワークの信頼できる発行局として、KMA では、すべてのストレージデバイスが登録および認証されること、そしてすべての暗号化鍵が規定のポリシーに従って作成、プロビジョニング、および削除されることが保証されます。
- **OKM GUI** − ワークステーション上で実行されるグラフィカルユーザーインタフェースであり、IP ネットワーク経由で KMA と通信して OKM を構成および管理します。OKM Manager GUI は、顧客が用意するワークステーションにインストールする必要があります。
- **OKM CLI** − OKM Manager GUI と同じ機能のサブセットをサポートする 2 つのコマンド行インタフェース (CLI) ユーティリティーです。これらの CLI によって、バックアップ、鍵のエクスポート、監査報告などのさまざまな作業の自動化が可能になります。
- **OKM クラスタ** − システム内の KMA の完全な集合。これらのすべての KMA は相互に認識し、情報を相互に複製します。
- **エージェント** − OKM クラスタによって管理される鍵を使用して、暗号化を実行するデバイスまたはソフトウェア。これらには、Oracle の StorageTek 暗号化テープドライブおよび Transparent Data Encryption (TDE) を備えた Oracle データベースサーバーが含まれます。

  エージェントは、エージェント API を介して KMA と通信します。エージェント API は、エージェントハードウェアまたはソフトウェアに組み込まれている一連のソフトウェアインタフェースです。

  注 − OKM での TDE の使用については、付録 B を参照してください。

OKM の概念

OKM クラスタ

OKM では複数の KMA のクラスタ化をサポートしており、これによって負荷分散とフェイルオーバーが実現されます。OKM クラスタ内のすべての KMA が、アクティブ / アクティブ方式で動作します。すべての KMA が、任意のエージェントにすべての機能を提供できます。ある KMA 上で実行された処理は、クラスタ内のほかのすべての KMA にただちに複製されます。

エージェント

エージェントは、暗号化操作を実行します。具体的には、書き込み時のデータの暗号化と読み取り時のデータの復号化を実行します。エージェントは、暗号化の実行に使用される鍵を作成したり、取得したりするために OKM クラスタと通信します。

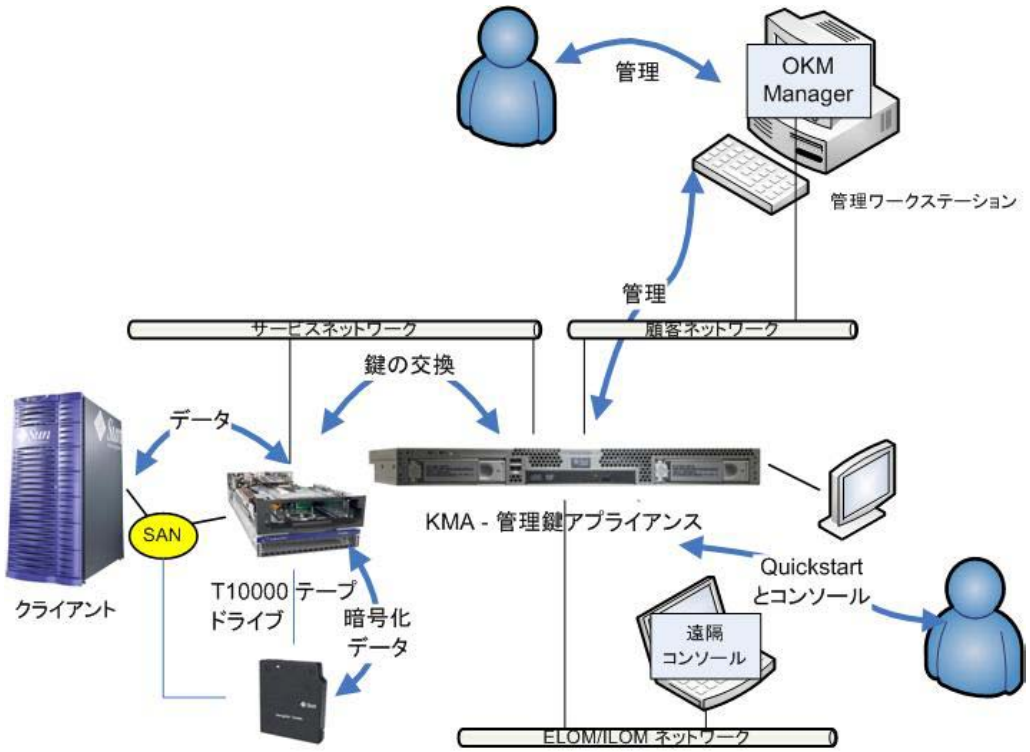
ネットワーク接続

OKM は、KMA、エージェント、および OKM Manager GUI が実行されているマシンの間の接続のために TCP/IP ネットワークを使用します。ネットワーク接続を柔軟に行うために、KMA には、ネットワーク接続用の次の 2 つのインタフェースが用意されています。

- 管理接続。顧客ネットワークへの接続を目的にしています。
- サービス接続。テープドライブへの接続を目的にしています。

本稼動の KMA インストール環境では、ライブラリ固有のアクセサリキットを利用できます。このアクセサリキットには、ドライブと KMA 間の接続に使用するスイッチおよびケーブルが含まれています。KMA との接続を図 1-1 に示します。

図 1-1 KMA との接続



初期設定 - 直接接続または遠隔コンソール

KMA の初期設定は、コンソール接続経由で実行します。この初期設定は、KMA に直接接続されたモニターとキーボードを使用するか、あるいは Embedded Lights Out Manager (ELOM) または Integrated Lights Out Manager (ILOM) の遠隔コンソール機能を使用して実行できます。ELOM または ILOM によってコンソールへの遠隔接続が提供されるため、サーバーの機能を実行できます。

ELOM/ILOM の遠隔コンソール機能には、3 つ目のネットワーク接続が必要です。図 1-1 では、「ELOM/ILOM ネットワーク」と示されています。遠隔コンソール機能を使用するには、40 ページの「サービスプロセッサを介した KMA へのアクセス」の説明に従って ELOM または ILOM の IP アドレスを構成する必要があります。

> **注 ー** 通常、ELOM/ILOM ネットワークは、実際には顧客ネットワークと同じネットワークです。

初期設定 ー QuickStart プログラム

出荷時のデフォルト状態にある KMA の電源を入れると、初期設定を実行するために、QuickStart と呼ばれるウィザード機能がコンソール上で実行されます。この処理が完了すると、その他のほとんどの機能を OKM Manager GUI から実行できるようになります。少数の機能に対しては、機能が制限されたコンソールインタフェースが有効なままです。

鍵のライフサイクル

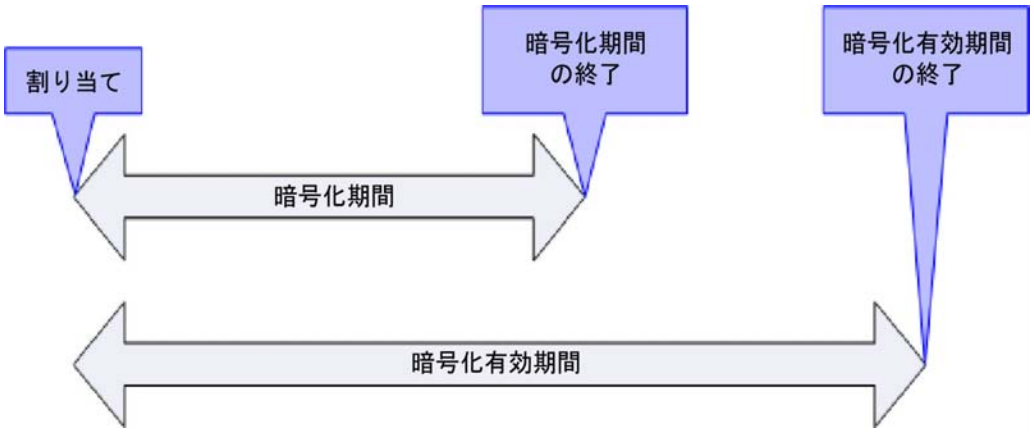
鍵のライフサイクルは、鍵ポリシーに基づいて行われます。OKM によって規定されるライフサイクルは、NIST 800-57 ガイドラインに基づいています。OKM の微妙な違いに対処するために、いくつかの状態が追加されています。

鍵のライフサイクルは、鍵ポリシーで定義されている次の 2 つの期間 (図 1-2 を参照) に基づいています。

- 暗号化期間
- 暗号化有効期間

暗号化期間は、データの暗号化に使用できる鍵が割り当てられてからの期間です。暗号化有効期間は、復号化に使用できる期間です。この 2 つの期間は、鍵が割り当てられたときに同時に開始されます。

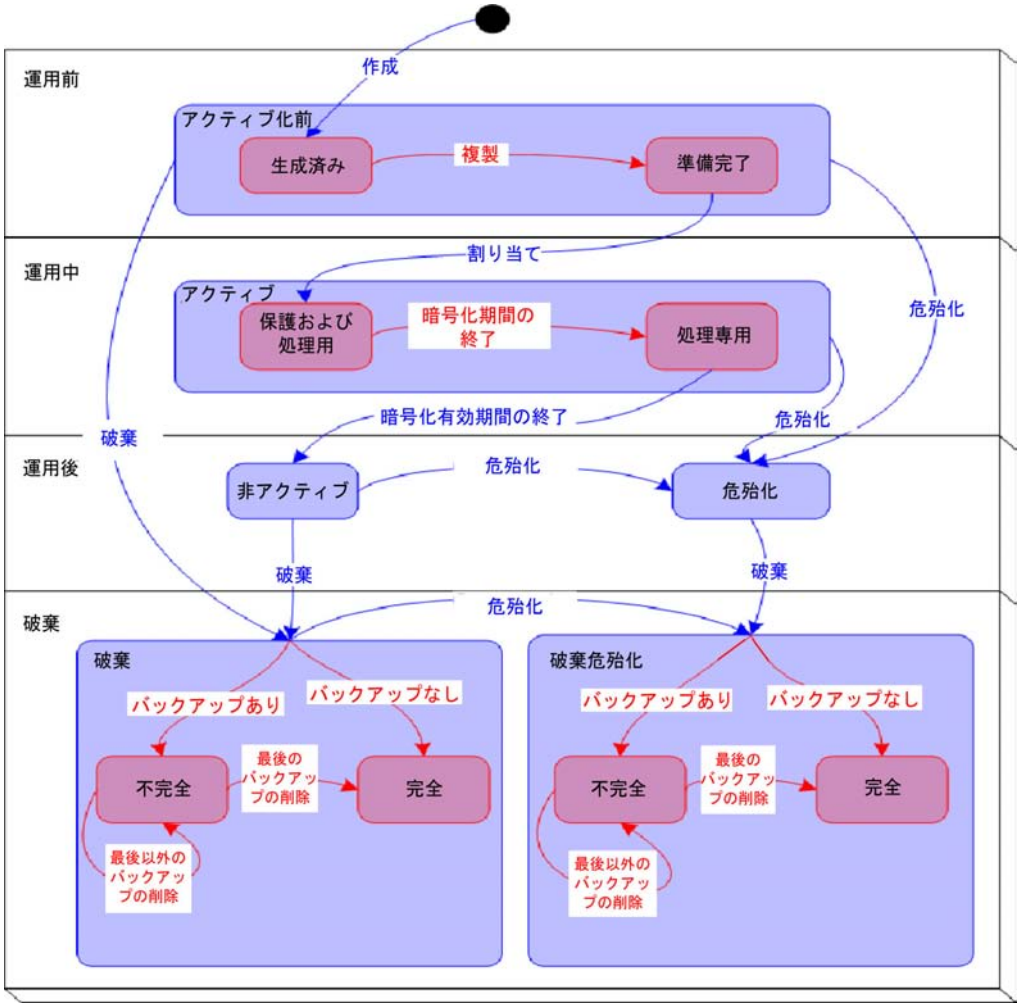
図 1-2 鍵のライフサイクル期間



状態遷移

暗号化期間と暗号化有効期間に、OKM のその他の機能が組み合わせられ、図 1-3 に示すような鍵の状態遷移が定義されます。この図で青色で示されている状態と遷移は、NIST 800-57 で定義されています。

図 1-3 状態遷移図



OKM 鍵の状態と遷移

図 1-3 で、赤色で示されている状態と遷移は OKM によって追加されたものです。OKM Manager で鍵を検査しているときは、もっとも内側の状態のみが示されます。OKM の状態を次に示します。

アクティブ化前 (Pre-activation)

この状態は、その鍵が生成されたが、まだ使用可能になっていないことを示します。アクティブ化前状態の中で、鍵はさらに、生成済みと準備完了という 2 つの状態を取ることができます。

生成済み (Generated)

生成済み状態は、OKM クラスタ内のいずれかの KMA 上で作成された鍵を示します。この状態の鍵は、マルチ OKM クラスタ内のほかの少なくとも 1 つの KMA に複製されるまで、生成済みのままになります。KMA が 1 つのみ存在するクラスタでは、鍵が生成済み状態から遷移するには、少なくとも 1 つのバックアップに記録される必要があります。

準備完了

準備完了状態は、その鍵が、複製またはバックアップによって損失から保護されていることを示します。準備完了状態の鍵は、割り当てに使用できます。「複製された」遷移は、その鍵が複製されたとき、または (単一 OKM クラスタの場合は) バックアップされたときに発生します。

アクティブ (Active)

この状態は、その鍵を情報の保護 (暗号化)、または以前に保護された情報の処理 (復号化) のために使用できることを示します。NIST では、アクティブな鍵を保護専用、処理専用、または保護および処理を行うために指定できることが示されています。さらに、対称データ暗号化鍵の場合は、特定の期間中は情報の保護および処理用として鍵を使用することができ、この期間が過ぎると鍵を引き続き処理専用として使用できることが明確に示されています。

OKM では、アクティブ状態の中に 2 つのサブ状態が追加されています。これらの状態は NIST に記載されていますが、状態として明確に識別されているわけではありません。

保護および処理 (Protect-and-process)

この状態の鍵は、暗号化と復号化の両方に使用できます。割り当てられた鍵は、この状態になります。暗号化エージェントが新しい鍵の作成を要求すると、割り当てが実行されます。

処理専用 (Process only)

この状態の鍵は、復号化には使用できますが、暗号化には使用できません。エージェントは、読み取り中または書き込み中の特定のデータユニットに対して使用可能な、保護および処理状態にある鍵が 1 つもないと判断すると、新しい鍵を作成します。

鍵が保護および処理状態から処理専用状態に移行するのは、その鍵の暗号化期間が終了したときのみです。

非アクティブ (Deactivated)

この状態は、その鍵が暗号化有効期間は過ぎているが、情報を処理 (復号化) するために引き続き必要になる可能性があることを示します。NIST では、この状態の鍵をデータの処理に使用できることが明確に示されています。

NIST ガイドラインでは、運用後鍵 (非アクティブ鍵や危殆化鍵を含む) をアクセス可能のままにしておく必要がある場合は、これらの鍵をアーカイブするべきであることが示されています。これは鍵の回復処理であり、鍵をアーカイブから再度呼び出して使用可能にすることができます。

OKM には、KMA バックアップの形式のアーカイブが用意されていますが、バックアップから 1 つの鍵を再度呼び出すことはできません。そのため、OKM では運用後のフェーズの鍵を OKM クラスタ内に保持し、エージェントからの要求があったときにこれらの鍵を提供します。

危殆化 (Compromised)

承認されていない実体に解放されるか、またはそのような実体によって検出された鍵は、危殆化状態にあります。危殆化状態の鍵は、情報を保護するために使用してはいけませんが、情報を処理するためには使用できます。

破棄 / 破棄危殆化

破棄状態の鍵と破棄危殆化状態の鍵 (破棄の前またはあとに危殆化された鍵) は存在しなくなります。ただし、その鍵に関する情報は保持できます。破棄された鍵の鍵データは、OKM クラスタから削除されます。破棄された鍵は、エージェントに提供されません。

> **注 ー** 鍵を破棄する唯一の方法は、GUI または管理 API を使用することです。

NIST ガイドラインでは、時間に基づいて鍵を破棄するための基準は提供されません。

OKM では、破棄状態と破棄危殆化状態の中に、不完全と完全という 2 つのサブ状態が定義されています。これらの状態は、OKM が作成するバックアップが OKM によって制御されないために作成されます。顧客の管理者は、バックアップが破棄されたら OKM に通知する必要があります。すべてのバックアップが破棄されたあとにのみ、実際に鍵が破棄されたと見なすことができます。

不完全 (Incomplete)

このサブ状態は、破棄された鍵を含むバックアップがまだ少なくとも 1 つ存在することを示します。このサブ状態では、その鍵は OKM クラスタ内のどの KMA にも存在しません。この状態の鍵をエージェントに提供することはできません。

Complete

このサブ状態は、その鍵を含むすべてのバックアップが破棄されたことを示します。鍵はどの KMA にもどのバックアップにも存在しません。厳密には、この鍵が含まれるバックアップがまだ存在している可能性があります。これらのバックアップは、破棄されたことが OKM によって識別されていますが、実際に破棄されたことを確認するのはユーザーの責任です。

破棄状態への遷移は、管理コマンドの実行結果としてのみ発生することに注意してください。また、鍵が非アクティブ状態または危殆化状態という運用後の段階である場合は、引き続き暗号化エージェントに提供することができます。この解釈は、運用後のフェーズに関する NIST の記述と整合性があります。NIST ガイドラインでは、運用後段階の鍵が「不要になった」場合には、これを破棄する必要があることが明確に示されています。Oracle では、鍵が「不要になった」時点を判定できるのはユーザーのみであるため、破棄状態への遷移を開始できるのは外部の実体のみであると考えています。

ユーザーと役割ベースのアクセス制御

OKM には、それぞれがユーザー ID とパスフレーズを持つ複数のユーザーを定義する機能があります。各ユーザーには、1 つ以上の事前定義済みの役割が付与されています。これらの役割は、次のとおりです。

- **セキュリティー責任者** – OKM の設定と管理を実行します。
- **オペレータ** – エージェントの設定と日常業務を実行します。
- **コンプライアンス責任者** – 鍵グループを定義し、それらの鍵グループへのエージェントからのアクセスを制御します。
- **バックアップオペレータ** – バックアップ操作を実行します。
- **監査者** – システムの監査証跡を表示できます。
- **定足数メンバー** – 保留中の定足数操作を表示して承認します。

セキュリティー責任者は、QuickStart 処理中に定義されます。QuickStart が完了したあと、OKM Manager GUI を使用して追加のユーザーを定義できます。

各役割に許可されている操作

表 1-3 に、役割ごとの機能のリストを示します。GUI とコンソールに対して許可される操作のみが示されます。操作が表示されていたとしても、それを実行しようとすると失敗する場合があります。この状況は、表示された時点と、その操作を実行しようとした時点の間で、役割がユーザーから削除された場合に発生することがあります。

監査者を除くすべての役割で、機能する暗号化システムを作成する必要があります。各ユーザーに 1 つまたは複数の役割を割り当てることができます。

定足数保護

OKM にはまた、特定の操作に対する定足数保護も用意されています。最大 10 ユーザーの定足数と、1 から定足数ユーザーの数までのしきい値を定義できます。この情報は鍵分割資格と呼ばれます (58 ページの「鍵分割資格の入力」を参照)。

そのユーザー ID とパスフレーズは、システムにログインするために使用されるユーザー ID とパスフレーズとは異なります。定足数の承認が必要な操作を実行しようとすると、すべての定足数ユーザーが各自のユーザー ID とパスフレーズを入力できる画面が表示されます。この操作が許可されるには、少なくとも指定されたしきい値のユーザー ID とパスフレーズを指定する必要があります。

データユニット、鍵、鍵グループ、および鍵ポリシー

データユニットは、エージェントによって暗号化されたデータを表すために使用されます。テープドライブの場合、データユニットはテープカートリッジであり、データユニットは常に存在しています。これは基本的な要件ではなく、将来的には、データユニットを定義しなくてもエージェントが動作する可能性があります。

鍵は、実際の鍵の値 (鍵データ) とその関連メタデータです。

鍵ポリシーは、鍵を制御するパラメータを定義します。これには、ライフサイクルパラメータ (暗号化期間と暗号化有効期間など) や、エクスポートまたはインポートパラメータ (たとえば、許可されたインポート、許可されたエクスポート) が含まれます。

鍵グループによって、鍵と鍵ポリシーが関連付けられます。鍵グループは特定の鍵ポリシーを含み、エージェントに割り当てられます。各エージェントには、許可された鍵グループのリストがあります。エージェントは、そのエージェントの許可された鍵グループのいずれかに割り当てられた鍵の取得のみを許可されます。エージェントにはまた、デフォルトの鍵グループもあります。エージェントが鍵を作成する (より具体的には、鍵をデータユニットに割り当てる) と、その鍵はそのエージェントのデフォルトの鍵グループに配置されます。エージェントによる鍵グループのより高度な制御を可能にするための機能が用意されています。ただし、既存のエージェントはこの機能を活用できません。

システムが機能するには、少なくとも 1 つの鍵ポリシーと 1 つの鍵グループが定義されている必要があります。その鍵グループは、すべてのエージェントのデフォルトの鍵グループとして割り当てられている必要があります。

TCP/IP 接続と KMA

各実体 (OKM Manager、エージェント、および同じクラスタ内のほかの KMA) と KMA の間にファイアウォールが存在する場合、そのファイアウォールでは、次のポート上での実体による KMA との TCP/IP 接続の確立が許可されている必要があります。

- OKM Manager から KMA への通信には、ポート 3331、3332、3333、3335 が必要です。
- エージェントから KMA への通信には、ポート 3331、3332、3334、3335 が必要です。
- KMA から KMA への通信には、ポート 3331、3332、3336 が必要です。

注 ー IPv6 アドレスを使用するように KMA を構成するユーザーの場合は、何らかの IPv6-over-IPv4 トンネル化トラフィックを使用したインターネットホストから内部ホストへのアクセスを防止するため、IPv4 ベースのエッジファイアウォールを、すべてのアウトバウンド IPv4 プロトコル 41 パケットと UDP ポート 3544 パケットをドロップするように構成します。

詳細については、ファイアウォール構成のマニュアルを参照してください。

表 1-1 に、KMA が明示的に使用するポート、または KMA によってサービスが提供されるポートを示します。

表 1-1 KMA のポート接続

ポート番号	Protocol	方向	説明
22	TCP	Listening	SSH (テクニカルサポートが有効になっている場合のみ)
123	TCP/UDP	Listening	NTP
3331	TCP	Listening	OKM CA サービス
3332	TCP	Listening	OKM 証明書サービス
3333	TCP	Listening	OKM 管理サービス
3334	TCP	Listening	OKM エージェントサービス
3335	TCP	Listening	OKM 検出サービス
3336	TCP	Listening	OKM 複製サービス

表 1-2 に、使用されていない可能性のあるポートで待機しているその他のサービスを示します。

表 1-2 その他のサービス

ポート番号	Protocol	方向	説明
53	TCP/UDP	接続	DNS (KMA が DNS を使用するように構成されている場合のみ)

表 1-2 その他のサービス

ポート番号	Protocol	方向	説明
68	UDP	接続	DHCP (KMA が DHCP を使用するように構成されている場合のみ)
111	TCP/UDP	Listening	RPC (KMA が rpcinfo クエリーに応答します)。このポートは、KMS 2.1 以前でのみ開かれます。
161	UDP	接続	SNMP (SNMP マネージャーが定義されている場合のみ)
546	UDP	接続	DHCPv6 (KMA が DHCP と IPv6 を使用するように構成されている場合のみ)
4045	TCP/UDP	Listening	NFS ロックデーモン (KMS 2.0 のみ)

注 ー

顧客がファイアウォール経由でサービスプロセッサの Web インタフェースや OKM コンソールにアクセスできるようにするには、ポート 443 が開いている必要があります。

ELOM および ILOM ポートを確認するには、『Oracle Key Manager Installation and Service Manual』を参照してください。

ネットワーク内の OKM

図 1-4 に、OKM ソリューションの標準的な配備を示します。

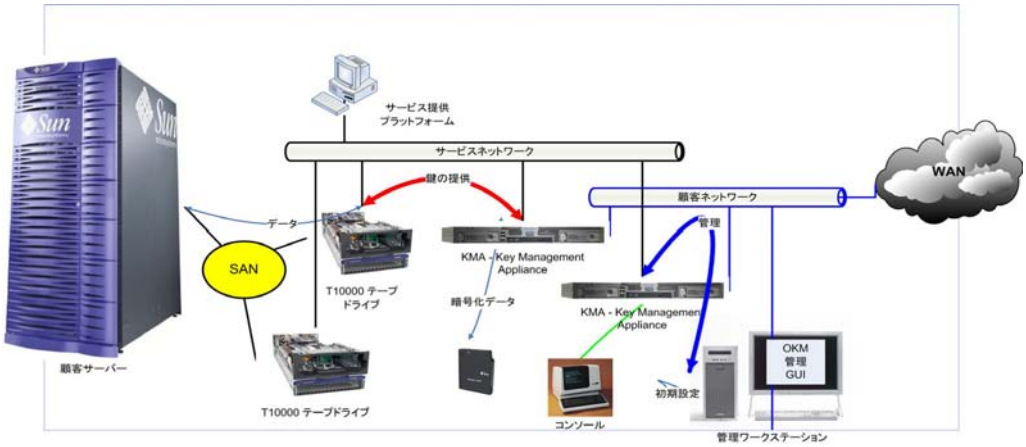


図 1-4 OKM ソリューションの標準的な配備

OKM Manager のソフトウェア要件

OKM Manager を実行するには、次のいずれかが動作するワークステーションが必要です。

- Solaris 10 10/09 (Update 8) x86
- Solaris 10 9/10 (Update 9) SPARC
- Solaris 10 9/10 (Update 9) x86
- Microsoft® Windows 7 Business
- Microsoft® Windows 7 Enterprise
- Microsoft® Windows Vista Business
- Microsoft® Windows XP Professional Version 2002
- Microsoft® Windows XP Professional
- Microsoft® Windows Server 2008 Version 6.0
- Microsoft® Windows Server 2003 R2 Standard Edition
- Microsoft® Windows Server 2003

GUI をインストールして起動するために、管理者 (Windows 上) またはルート (Solaris 上) 権限を持っている必要はありません。

オンラインヘルプの使用法

OKM Manager には、包括的なオンラインヘルプが含まれています。OKM Manager の任意の画面でヘルプを表示するには、次の手順を実行します。

- パネルの上部にある「**Help**」ボタンをクリックして、全般的なヘルプを表示します。

または

- **Tab** キーを押すか、またはパネル内の任意の場所をクリックして、パネルに移動します。次に、**F1** キーを押して、コンテキストヘルプを表示します。

役割ベースのアクセス制御

OKM では、次の役割が定義されています。

- **セキュリティー責任者** – セキュリティー設定、ユーザー、サイト、および転送パートナーを管理します。
- **コンプライアンス責任者** – 鍵ポリシーと鍵グループを管理し、鍵グループを使用できるエージェントと転送パートナーを決定します。
- **オペレータ** – エージェント、データユニット、および鍵を管理します。
- **バックアップオペレータ** – バックアップを実行します。
- **監査者** – OKM クラスタに関する情報を表示します。
- **定足数メンバー** – 保留中の定足数操作を表示して承認します。

単一 KMA ユーザーアカウントでは、1 つ以上の役割にメンバーシップを割り当てることができます。KMA では、ユーザーの役割に基づいて、要求元のユーザー実体に操作を実行する権限があるかどうかが確認されます。役割については、348 ページの「KMA へのログイン」を参照してください。

役割ベースの操作

表 1-3 に、各ユーザーの役割で実行できるシステムの操作を示します。「役割」列の内容は、次のとおりです。

- **はい** ― この役割は操作の実行を許可されています。
- **定足数** ― この役割は操作の実行を許可されていますが、定足数も提供する必要があります。
- 空白は、この役割が操作の実行を許可されていないことを示します。

表 1-3 システムの操作とユーザーの役割

		役割					
実体	**操作**	**セキュリティー責任者**	**コンプライアンス責任者**	**オペレータ**	**バックアップオペレータ**	**監査者**	**定足数メンバー**
コンソール							
	ログイン	はい	はい	はい	はい	はい	はい
	KMA ロケールの設定	はい					
	KMA IP アドレスの設定	はい					
	技術サポートの有効化	はい					
	技術サポートの無効化	はい		はい			
	主管理者の有効化	はい					
	主管理者の無効化	はい		はい			
	KMA の再起動			はい			
	KMA の停止			はい			
	クラスタへの OKM のログイン	定足数					
	Set User's Passphrase	はい					
	KMA のリセット	はい					
	KMA のゼロ化	はい					
	ログアウト	はい	はい	はい	はい	はい	はい
接続							
	ログイン	はい	はい	はい	はい	はい	はい
	プロファイルの作成	はい	はい	はい	はい	はい	はい

表 1-3 システムの操作とユーザーの役割

実体	操作	役割 セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
	プロファイルの削除	はい	はい	はい	はい	はい	はい
	構成設定の設定	はい	はい	はい	はい	はい	はい
	切断	はい	はい	はい	はい	はい	はい
鍵分割資格							
	一覧表示	はい					
	変更	定足数					
自律ロック解除							
	一覧表示	はい					
	変更	定足数					
KMA のロック / ロック解除							
	状態の一覧表示	はい	はい	はい	はい	はい	
	ロック	はい					
	ロック解除	定足数					
サイト							
	作成	はい					
	一覧表示	はい		はい			
	変更	はい					
	削除	はい					
セキュリティーパラメータ							
	一覧表示	はい	はい	はい	はい	はい	
	変更	はい					
KMA							
	作成	定足数					
	一覧表示	はい		はい			
	変更	定足数					
	削除	はい					
ユーザー							
	作成	定足数					
	一覧表示	はい					
	変更	はい					

表 1-3 システムの操作とユーザーの役割

実体	操作	役割 セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
	パスフレーズの変更	定足数					
	削除	はい					
役割							
	追加	定足数					
	一覧表示	はい					
鍵ポリシー							
	作成		はい				
	一覧表示		はい				
	変更		はい				
	削除		はい				
鍵グループ							
	作成		はい				
	一覧表示		はい	はい			
	データユニットの一覧表示		はい	はい			
	エージェントの一覧表示		はい	はい			
	変更		はい				
	削除		はい				
エージェント							
	作成			はい			
	一覧表示		はい	はい			
	変更			はい			
	パスフレーズの変更			はい			
	削除			はい			
エージェント / 鍵グループの割り当て							
	一覧表示		はい	はい			
	変更		はい				
データユニット							
	作成						
	一覧表示		はい	はい			

表 1-3 システムの操作とユーザーの役割

実体	操作	役割					
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
	変更			はい			
	鍵グループの変更		はい				
	削除						
鍵							
	データユニット鍵の一覧表示		はい	はい			
	破棄			はい			
	危殆化		はい				
転送パートナー							
	構成	定足数					
	一覧表示	はい	はい	はい			
	変更	定足数					
	削除	はい					
鍵転送鍵							
	一覧表示	はい					
	更新	はい					
転送パートナー鍵グループの割り当て							
	一覧表示		はい	はい			
	変更		はい				
バックアップ							
	作成				はい		
	一覧表示	はい	はい	はい	はい		
	破棄された鍵を含むバックアップの一覧表示		はい	はい			
	復元	定足数					
	破棄の確認				はい		
コアセキュリティーバックアップ							
	作成	はい					
SNMP マネージャー							
	作成	はい					
	一覧表示	はい		はい			

表 1-3 システムの操作とユーザーの役割

実体	操作	役割					
		セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
	変更	はい					
	削除	はい					
イベントの監査							
	表示	はい	はい	はい	はい	はい	
	エージェント履歴の表示		はい	はい			
	データユニット履歴の表示		はい	はい			
	データユニット鍵履歴の表示		はい	はい			
システムダンプ							
	作成	はい		はい			
システム時刻							
	一覧表示	はい	はい	はい	はい	はい	
	変更	はい					
NTP サーバー							
	一覧表示	はい	はい	はい	はい	はい	
	変更	はい					
ソフトウェアバージョン							
	一覧表示	はい	はい	はい	はい	はい	
	アップグレード			定足数			
ネットワーク構成							
	表示	はい	はい	はい	はい	はい	
保留中の定足数操作							
	承認						定足数
	削除	はい					

Key Management Appliance の設定および管理

OKM ソリューションをインストールして構成する手順については、『OKM 2.4 Installation and Service Manual』を参照してください。

ASR (Auto Service Request) 機能

ASR (Auto Service Request) は、特定のハードウェア障害が発生したときに Oracle サービスを自動的に要求するように設計された、システムおよび Oracle/Sun 限定保証のための Oracle Premier Support の機能です。

ASR は、ハードウェア障害が発生したときに Oracle サービスへの連絡を開始する必要をなくし、必要な通話の数と、必要な通話時間全体の両方を削減することによって、問題をより迅速に解決するように設計されています。ASR ではまた、電子的な診断データの活用によって、サポート操作も単純化されます。ASR はインストールと配備が容易であり、セキュリティーを保証するために完全にユーザーによって制御されます。

ASR を有効にするには、233 ページの「ASR (Auto Service Request)」を参照してください。セキュリティー責任者の役割のアクセス権が必要です。

追加のドキュメントは、次の URL で参照できます。

http://www.oracle.com/technetwork/server-storage/asr/documentation/index.html

Sun システムのための Oracle Auto Service Request の Web サイトは次のとおりです。

http://www.oracle.com/us/support/systems/premier/auto-service-request-155415.html

2

はじめに

この章では、次の項目について説明します。

- サービスプロセッサを介した KMA へのアクセス ー Embedded Lights Out Manager (ELOM) と Integrated Lights Out Manager (ILOM) によって、コンソールへの遠隔接続が提供されます (40 ページ)。
- QuickStart プログラムの実行 ー QuickStart は、顧客 (セキュリティー責任者または資格のある代理人) が新しい KMA を構成するために使用できるユーティリティーです (49 ページ)。

  注 ー サービス担当者も QuickStart を実行できますが、このプログラムでは重要なセキュリティーパラメータが確立されるため、顧客は企業のセキュリティーポリシーに従って、自分で実行するように選択する可能性があります。

サービスプロセッサを介した KMA へのアクセス

Embedded Lights Out Manager (ELOM) と Integrated Lights Out Manager (ILOM) には、メインサーバーとは別のサービスプロセッサが搭載されています。これらのサービスプロセッサによって KMA への遠隔接続が提供されるため、*QuickStart* プログラムなどのサーバーの機能を実行できます。

注 –
Sun Fire X2100 または X2200 サーバーである KMA がサービスプロセッサとして ELOM を使用しているのに対して、Sun Fire X4170 M2 サーバーである KMA はサービスプロセッサとして ILOM を使用しています。

構成情報については、『Embedded Lights Out Manager Administration Guide』または『Integrated Lights Out Manager Web Interface Procedures Guide』を参照してください。

KMA への接続

ELOM または ILOM を介した KMA への接続には、次のいずれかを使用します。

- LAN 1 NET MGT ELOM または ILOM インタフェースによるネットワーク接続 (推奨)
- KMA に接続されているキーボードとモニター

ポップアップブロッカによって、Windows での次の手順による起動ができなくなります。手順を開始する前に、ポップアップブロッカを無効にしてください。

ウィンドウは表示されるが、コンソールウィンドウが表示されない場合は、Web ブラウザまたは Java バージョンとサービスプロセッサに互換性がありません。ブラウザと Java を最新版にアップグレードしてください。互換性のあるバージョンの一覧は、表 2-1 を参照してください。

表 2-1 サポートされている ELOM 互換の Web ブラウザおよび Java バージョン

クライアント OS	サポートされている Web ブラウザ	Java Runtime Environment (Java Web Start を含む)
• Microsoft Windows XP • Microsoft Windows 2003 • Microsoft Windows Vista	• Internet Explorer 6.0 以降 Mozilla 1.7.5 以降 • Mozilla Firefox 1.0	JRE 1.5 (Java 5.0 Update 7 以降)
• Red Hat Linux 3.0 および 4.0	• Mozilla 1.7.5 以降 • Mozilla Firefox 1.0	
• Solaris 9 • Solaris 10 • Solaris Sparc • SUSE Linux 9.2	• Mozilla 1.7.5	

表 2-1 サポートされている ELOM 互換の Web ブラウザおよび Java バージョン

Java Runtime Environment 1.5 は、http://java.com からダウンロードできます。 ELOM マニュアルの最新バージョンは次で参照できます。 http://docs.oracle.com/cd/E19121-01/sf.x2200m2/819-7544-11/819-7544-11.pdf

表 2-2 サポートされている ILOM 互換の Web ブラウザおよび Java バージョン

クライアント OS	サポートされている Web ブラウザ	Java Runtime Environment (Java Web Start を含む)
• Microsoft Windows 98 • Microsoft Windows 2000 • Microsoft Windows XP • Microsoft Windows Vista	• Internet Explorer 6.0 以降 • Mozilla 1.7.5 以降 • Mozilla Firefox 1.0 以降 • Opera 6.x 以降	JRE 1.5 (Java 5.0 Update 7 以降)
• Linux (Red Hat、SuSE、Ubuntu)	• Mozilla 1.7.5 以降 • Mozilla Firefox 1.0 以降 • Opera 6.x 以降	
• Solaris 9 • Solaris 10	• Mozilla 1.7.5 以降 • Firefox 1.0 以降	
Java Runtime Environment 1.5 は、http://java.com からダウンロードできます。 ILOM マニュアルの最新バージョンは次で参照できます。 http://download.oracle.com/docs/cd/E19860-01/index.html		

ネットワーク接続の使用 - ELOM

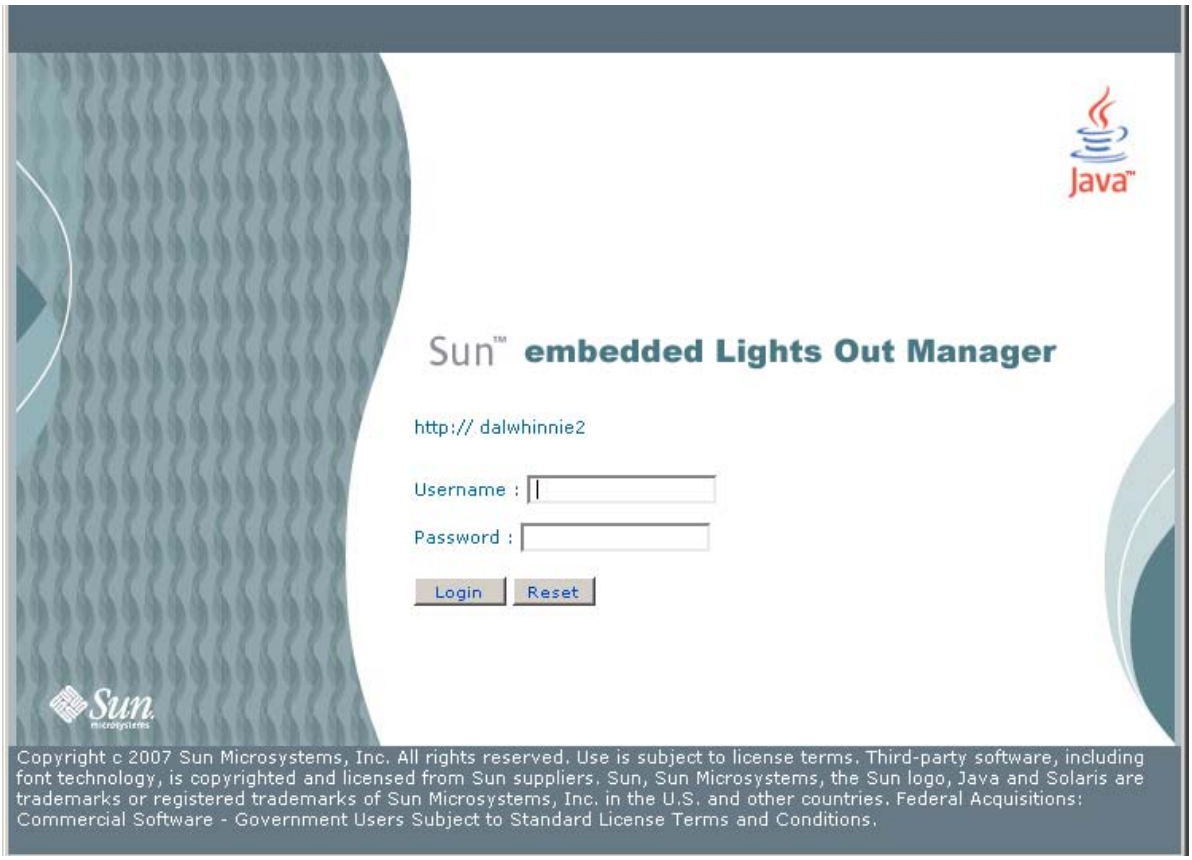
1. ネットワーク上の別のワークステーションを使用して、Web ブラウザを起動します。
2. LAN 1 (NET MGT) の IP アドレスまたはホスト名 (構成したばかりのアドレス) を使用して KMA ELOM に接続します。

   注 ー ELOM に含まれている証明書が、割り当てられた名前または IP と一致しないため、Web ブラウザに 1 つ以上の警告が表示されます。

3. 「**OK**」または「**Yes**」をクリックして、これらの警告を無視します。

   警告を無視したあと、ELOM のログインプロンプトが表示されます。

図 2-1 Embedded Lights Out Manager のログイン画面



4. ユーザー ID に `root`、パスワードに `changeme` を使用してログインします。

   次に表示される画面は Manager の画面です。サーバーを接続しただけで、まだサーバーの電源が入っていない場合、システムの起動は完了していません。

   KMA は、最初の電源投入時に自動的に起動するように構成されており、電源投入から数分で起動して QuickStart プロンプトが表示されるはずです。

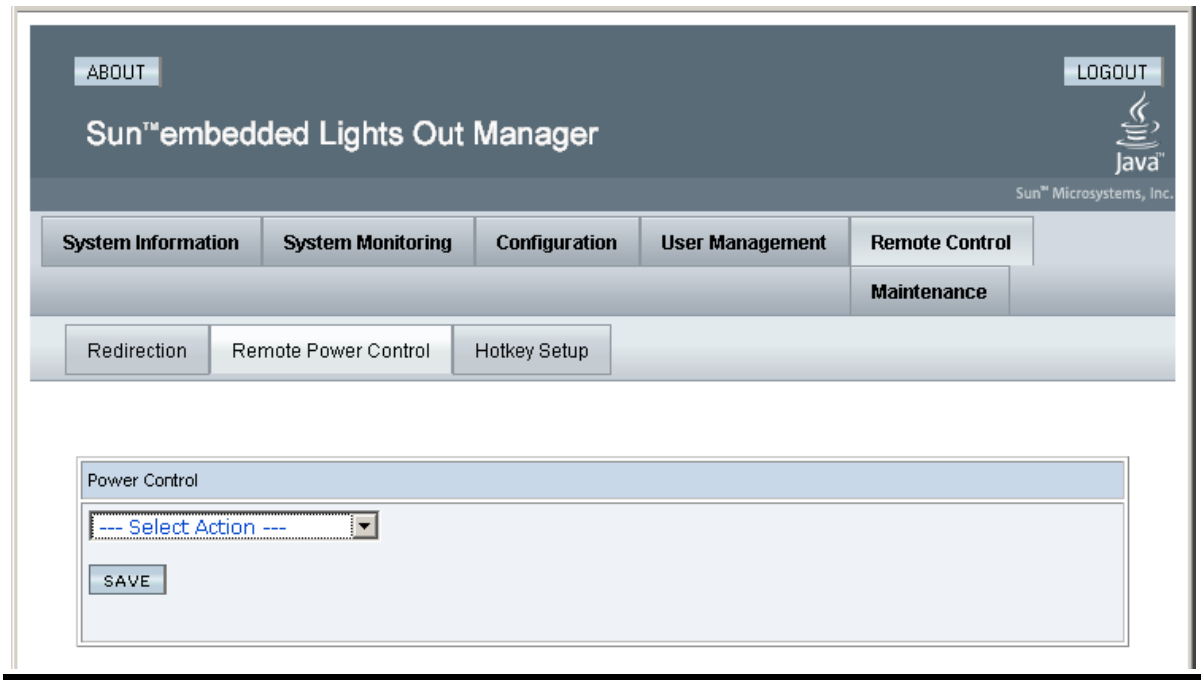
5. 「**System Monitoring**」タブをクリックして、電源の状態を確認します。

6. 「Power Status」が「power off」を示している場合は、上側のタブ行の右端にある「**Remote Control**」タブをクリックします。

7. 2 番目のタブ行にある「**Remote Power Control**」タブをクリックします。

8. 「Select Action」ドロップダウンで「**Power On**」を選択し、「**Save**」ボタンをクリックします。
   KMA の電源投入が開始されます。この処理には数分かかりますが、その間も KMA の構成を続行できます。

図 2-2 電源制御



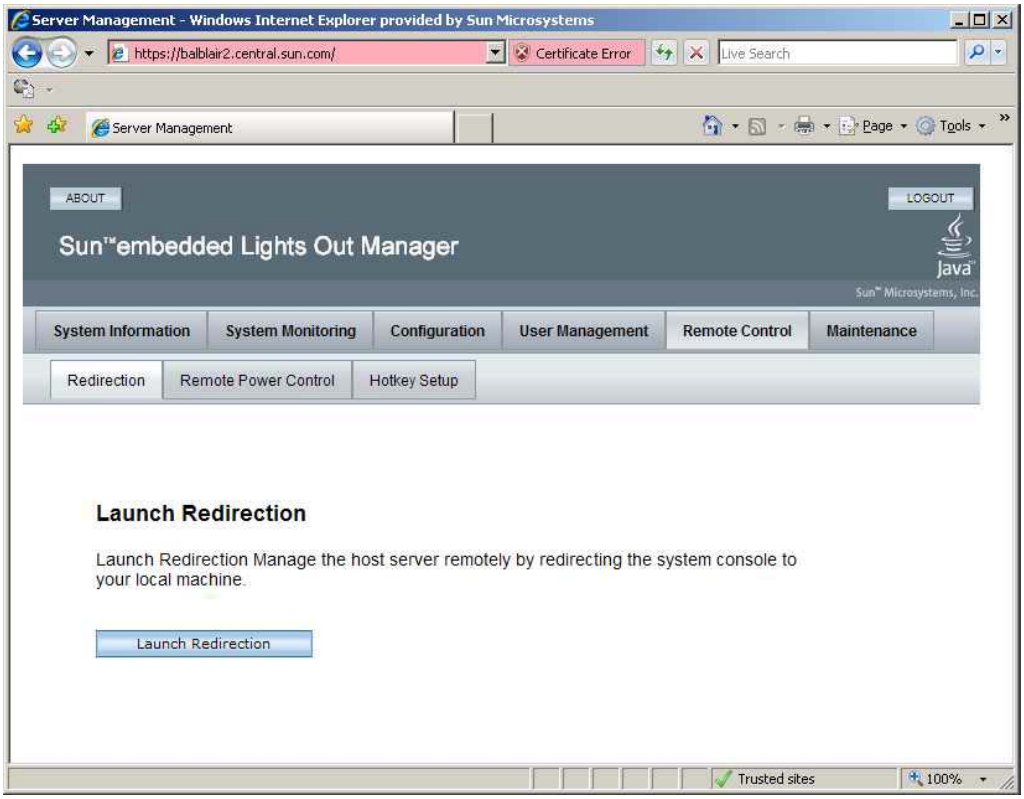
9. 先頭のタブ行にある「**Remote Control**」タブをクリックします。

10. 2 番目のタブ行にある「**Redirection**」タブをクリックします。

11. 「**Launch Redirection**」ボタンをクリックします。

遠隔コンソールウィンドウの起動前に、Java アプレットがダウンロードされます。

図 2-3 リダイレクションの起動 (ELOM)



ここで、新しいウィンドウに遠隔コンソール画面が表示されます。

12. javaRKVM.jnlp ファイルが要求された場合は、これを保存してから開き、遠隔コンソールを起動します。表示されている警告があった場合は、それらをすべてクリックして無視します。
13. 次の処理手順を実行するには、48 ページの「OKM コンソールの起動」に進みます。

ネットワーク接続の使用 - ILOM

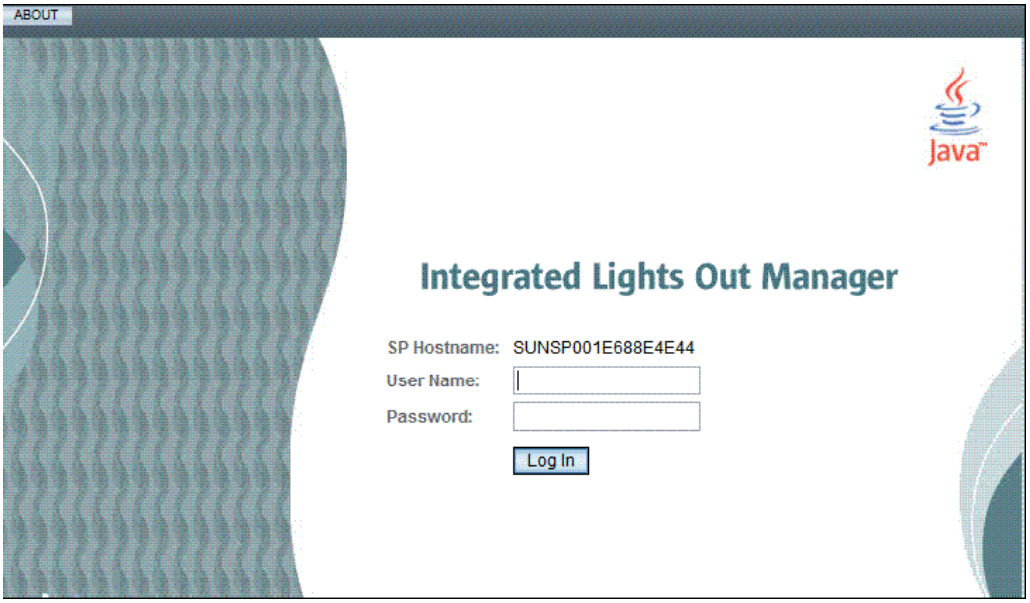
1. ネットワーク上の別のワークステーションを使用して、Web ブラウザを起動します。
2. LAN 1 (NET MGT) の IP アドレスまたはホスト名 (構成したばかりのアドレス) を使用して KMA ILOM に接続します。

   注 ー ILOM に含まれている証明書が、割り当てられた名前または IP と一致しないため、Web ブラウザに 1 つ以上の警告が表示されます。

3. 「**OK**」または「**Yes**」をクリックして、これらの警告を無視します。

   警告を無視したあと、ILOM のログインプロンプトが表示されます。

図 2-4 Integrated Lights Out Manager のログイン画面



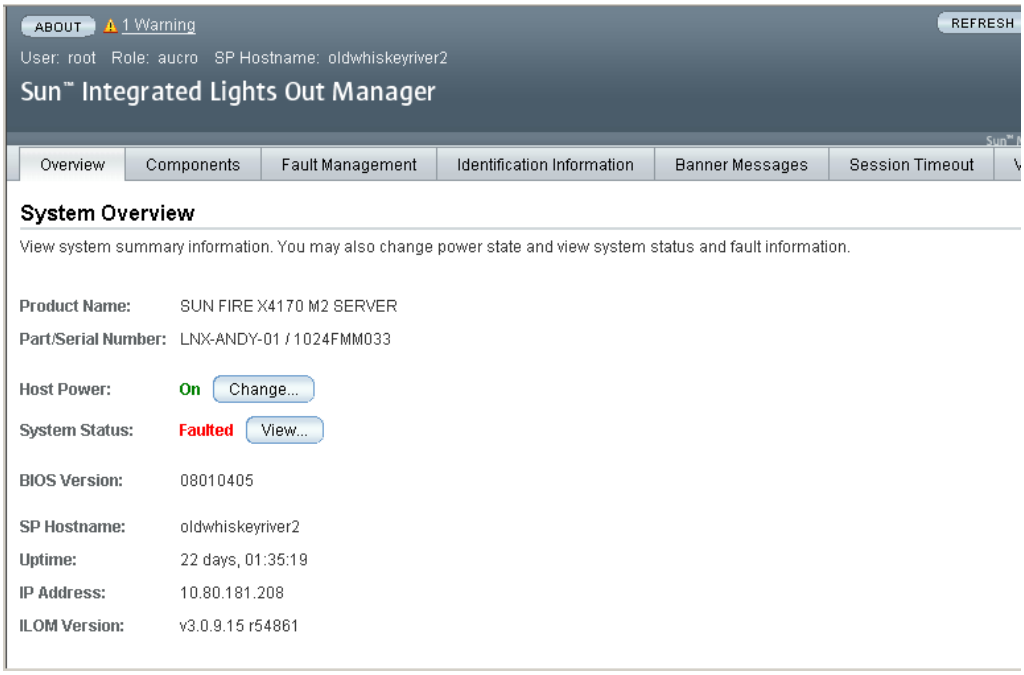
4. ユーザー ID に `root`、パスワードに `changeme` を使用してログインします。

   次に表示される画面は Manager の画面です。サーバーを接続しただけで、まだサーバーの電源が入っていない場合、システムの起動は完了していません。

   KMA は、最初の電源投入時に自動的に起動するように構成されており、電源投入から数分で起動して QuickStart プロンプトが表示されるはずです。

5. 「Host Power」の横に表示されている電源の状態を確認します。

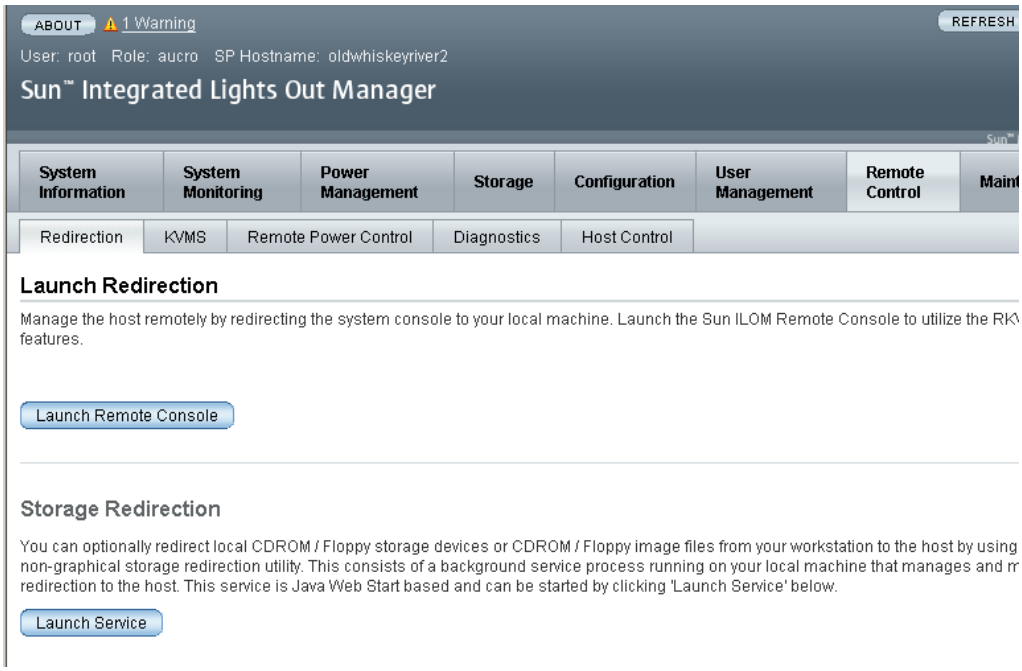
図 2-5 電源制御



6. 「Host Power」が電源切断を示している場合は、「**Change**」ドロップダウンをクリックします。
7. 「Select Action」ドロップダウンで「**Power On**」を選択し、「**Save**」ボタンをクリックします。
   KMA の電源投入が開始されます。この処理には数分かかりますが、KMA の構成を続行することができます。
8. 先頭のタブ行にある「**Remote Control**」タブをクリックします。

9. 2 番目のタブ行にある「Redirection」タブをクリックします。

図 2-6 リダイレクションの起動 (ILOM)



10.「**Launch Remote Console**」ボタンをクリックします。

遠隔コンソールウィンドウの起動前に、Java アプレットがダウンロードされます。ここで、新しいウィンドウに遠隔コンソール画面が表示されます。

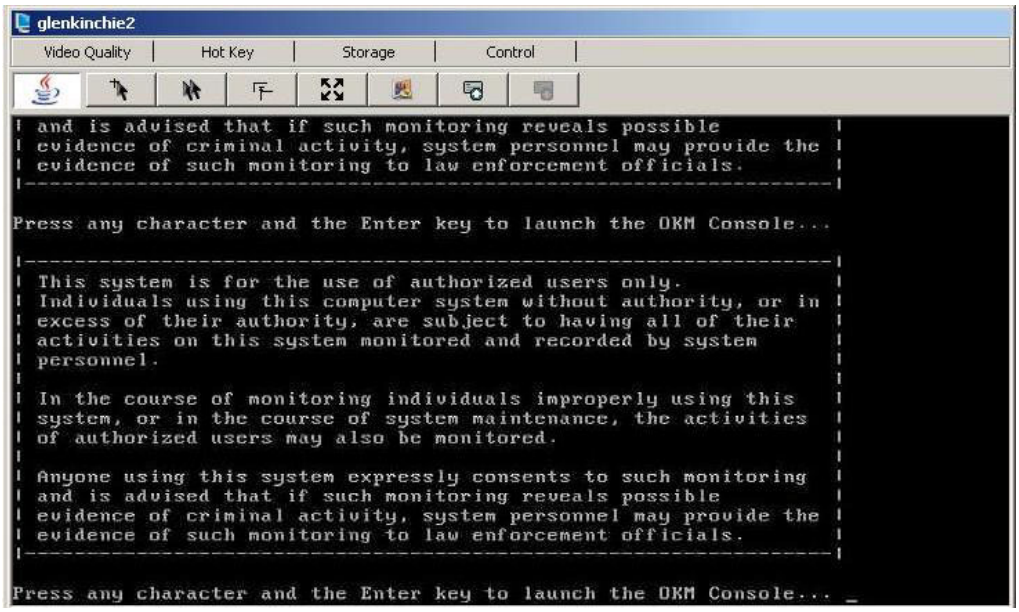
11. javaRKVM.jnlp ファイルが要求された場合は、これを保存してから開き、遠隔コンソールを起動します。表示されている警告があった場合は、それらをすべてクリックして無視します。

12. 次の処理手順を実行するには、48 ページの「OKM コンソールの起動」に進みます。

OKM コンソールの起動

1. 任意のキーを押し、Enter キーを押して続行します。KMA が SCA 6000 カードをチェックし、そのステータスを報告します。

図 2-7 遠隔コンソール



2. Enter キーを押します。

ここで、50 ページの「QuickStart の起動」で説明されている QuickStart プログラムプロンプトに進みます。

QuickStart プログラムの実行

出荷時のデフォルト状態にある KMA の電源を入れると、QuickStart と呼ばれる特殊なモードの KMA 構成メニューが自動的に実行されます。QuickStart によって、KMA の初期化に必要な最低限の構成情報が収集されます。QuickStart プログラムの実行がいったん正常に完了すると、このプログラムは再度実行できません。再度 QuickStart プログラムにアクセスするには、KMA を出荷時のデフォルト状態にリセットするしか方法はありません (371 ページの「KMA の出荷時のデフォルトへのリセット」を参照)。

注 ー 以降の画面例では、太字のエントリがユーザーから応答する領域を表しています。

QuickStart の起動

QuickStart を実行するには、次の手順を実行します。

KMA の電源を入れます。KMA の電源をはじめて入れると、QuickStart が実行され、「Welcome to QuickStart!」画面が表示されます。

```
Copyright (c) 2007, 2011, Oracle and/or its affiliates. All
rights reserved.
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Welcome to QuickStart!

The QuickStart program will guide you through
the necessary steps for configuring the KMA.

You may enter Ctrl-c at any time to abort; however,
it is necessary to successfully complete all steps in this
initialization program to enable the KMA.

Press Enter to continue:

Set Keyboard Layout
_____________________________________________________________

Press Ctrl-c to abort.

You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian          ( 2) Belarusian    ( 3) Belgian
( 4) Bulgarian         ( 5) Croatian      ( 6) Danish
( 7) Dutch             ( 8) Finnish       ( 9) French
(10) German            (11) Icelandic     (12) Italian
(13) Japanese-type6    (14) Japanese      (15) Korean
(16) Malta_UK          (17) Malta_US      (18) Norwegian
(19) Portuguese        (20) Russian       (21) Serbia-And-
                                               Montenegro
(22) Slovenian         (23) Slovakian     (24) Spanish
(25) Swedish           (26) Swiss-French  (27) Swiss-German
(28) Taiwanese         (29) TurkishQ      (30) TurkishF
(31) UK-English        (32) US-English

The current layout is US-English.

Please enter the number for the keyboard layout : 32

The keyboard layout has been applied successfully.

Press Enter to continue:
```

注 ー Ctrl-c キーを押すと、QuickStart プログラムがリセットされ、「Welcome to QuickStart!」画面が再度表示されます。

ネットワーク構成の指定

次の手順を使用すると、ネットワーク構成を確立できます。

KMA の管理 IP アドレスの設定

KMA の管理 IP アドレスを設定するには、次の手順を実行します。

1. Enter キーを押して続行します。次の情報が表示されます。

```
Set KMA Management IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.


Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

Do you want to use DHCP to configure the Management Network
interface? [y/n]:

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:
```

2. メインメニューの「`Please enter your choice:`」プロンプトで、**3** を入力して Enter キーを押します。
3. 「`Do you want to configure the Management Network interface to have an IPv6 address`」プロンプトで、**n** または **y** のいずれかを入力します。
4. 「**Do you want to use DHCP to configure the Management Network interface**」プロンプトで、**n** または y のいずれかを入力します。**n** を入力した場合は、手順 5 に進みます。**y** を入力した場合は、手順 53 ページの「KMA のサービス IP アドレスの設定」に進みます。
5. プロンプトで、管理ネットワークの IP アドレスを入力して Enter キーを押します。
6. 「`Please enter the Management Network Subnet Mask: `」プロンプトで、サブネットマスクアドレス (255.255.254.0 など) を入力して Enter キーを押します。

技術サポートアカウントの有効化

技術サポートアカウントを有効にするには、次の手順を実行します。

1. Enter キーを押して続行します。次の情報が表示されます。

```
To assist in troubleshooting your network configuration,
you might want to enable the technical support account for the
network configuration steps of the QuickStart process.

Do you want to enable this support account for the network
configuration steps of the QuickStart process? [y/n]: y

Press Enter to continue:
```

2. QuickStart で技術サポートアカウントを有効にする場合は、「`Do you want to enable this support account for the network configuration steps of the QuickStart process?`」プロンプトで **y** を入力します。それ以外の場合は、**n** を入力し、手順 3 に進みます。

   注 ー y を入力した場合は、373 ページの「技術サポートアカウントの有効化」で説明したのと同じプロンプトが表示されます。これらのプロンプトに応答したあと、手順 3 に進みます。

3. Enter キーを押して続行します。

   注 ー 技術サポートアカウントを有効にした場合は、56 ページに示されている「DNS 設定の指定」の処理を完了したあと、QuickStart がそのアカウントを無効にします。次の画面が表示されます。

```
The support account is now being disabled.

Technical Support configuration changes have been completed.

Press Enter to continue:
```

KMA のサービス IP アドレスの設定

KMA のサービス IP アドレスを設定するには、次の手順を実行します。

1. Enter キーを押して続行します。次の情報が表示されます。

```
Set KMA Service IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.


Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]: y

Do you want to use DHCP to configure the Service Network interface?
[y/n]: n

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:
```

2. メインメニューの「Please enter your choice:」プロンプトで、**4** を入力して Enter キーを押します。
3. 「Do you want to configure the Service Network interface to have an IPv6 address」プロンプトで、**n** または **y** のいずれかを入力します。
4. 「Do you want to use DHCP to configure the Service Network interface」プロンプトで、**n** または y のいずれかを入力します。**n** を入力した場合は、手順 5 に進みます。**y** を入力した場合は、手順 54 ページの「ゲートウェイの表示 / 追加 / 削除」に進みます。
5. プロンプトで、サービスネットワークの IP アドレスを入力して Enter キーを押します。
6. 「Please enter the Service Network Subnet Mask:」プロンプトで、サブネットマスクアドレス (255.255.255.0 など) を入力して Enter キーを押します。

ゲートウェイの表示 / 追加 / 削除

このメニューオプションは、管理 (M) およびサービス (S) インタフェース上の現在のゲートウェイ設定 (1 ページあたり 5 個) を表示します。

1. Enter キーを押して続行します。次の情報が表示され、ゲートウェイの追加、ゲートウェイの削除、現在のゲートウェイ構成の受け入れのいずれかを実行できることが示されます。

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
   1 default                    10.80.181.254               0.0.0.0         M
   2 default                    10.80.181.21                0.0.0.0         M
   3 default                    192.168.1.119               0.0.0.0         S
   4 10.0.0.0                   10.80.180.25                255.255.254.0   M
*  5 10.80.180.0                10.80.180.39                255.255.254.0   M

Press Enter to continue:

Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
*  6 192.168.1.0                192.168.1.39                255.255.255.0   S
   7 192.168.25.0               10.80.180.25                255.255.255.0   M
   8 192.168.26.0               10.80.180.25                255.255.255.0   M
*  9 127.0.0.1                  127.0.0.1                   255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6    10              M

(1) Continue
(2) Back
1
```

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
* 11 fe80::                     fe80::216:36ff:feca:15b9    10              S

You can add a route, delete a route, or exit the gateway configuration.
Please choose one of the following:

(1)  Add a gateway
(2)  Remove a configured gateway (only if modifiable)
(3)  Exit gateway configuration
(4)  Display again
3
```

2. メインメニューの「`Please enter your choice:`」プロンプトで、**5** を入力して Enter キーを押します。
3. 「`(1) Continue (2) Back`」プロンプトで、**1** を入力して次のゲートウェイ設定を表示するか、または 2 を入力して以前のゲートウェイ設定に戻ります。
4. 「`Please choose one of the following:`」プロンプトで、**1**、**2**、**3**、または **4** を入力して Enter キーを押します。

注 ー 任意の時点で Ctrl+c キーを押すと、変更は保存されずにメインメニューに戻ります。

DNS 設定の指定

このメニューオプションは DNS 設定を表示するとともに、新しい DNS ドメイン (新しい DNS ドメインを構成する場合) と DNS サーバーの IP アドレスの入力を求めるプロンプトを表示します。

1. Enter キーを押して続行します。次の情報が表示されます。

```
Set DNS Configuration
------------------------------------------------------------

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain:
Nameservers:

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:
```

2. メインメニューの「`Please enter your choice:`」プロンプトで、**6** を入力して Enter キーを押します。
3. 「`Please enter the DNS Domain (blank to unconfigure DNS):`」プロンプトで、DNS ドメイン名を入力します。
4. 「`Please enter DNS Server IP address`」プロンプトで、DNS サーバーの IP アドレスを入力します。最大で 3 つの IP アドレスを入力できます。
5. IP アドレスを指定しないで終了するには、`Enter` キーを押します。

KMA の初期化

1. Enter キーを押して続行します。次の情報が表示されます。

```
The KMA Name is a unique identifier for your KMA. This name
should not be the same as the KMA Name for any other KMA in
your cluster. It also should not be the same as any User
Names or Agent IDs in your system.

Please enter the KMA Name: KMA-1

Press Enter to continue:
```

2. プロンプトで、KMA の一意の識別子を入力します。

> **注 ー** QuickStart プログラムを使用して一度設定した KMA 名は、変更することができません。変更する唯一の方法は、KMA を出荷時のデフォルトにリセットして、QuickStart を再度実行することです。

クラスタの構成

1. プロンプトで、Enter キーを押します。次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can
have this KMA join an existing Cluster. You can also restore
a backup to this KMA or change the KMA Version.

Please choose one of the following:
(1) Create New Cluster
(2) Join Existing Cluster
(3) Restore Cluster from Backup

Please enter your choice: 1

Create New Cluster
```

2. プロンプトで、**1**、**2**、または **3** を入力して Enter キーを押します。

1 を入力した場合は、58 ページの「鍵分割資格の入力」へ進みます。

2 を入力した場合は、65 ページの「既存のクラスタへの参加」へ進みます。

3 を入力した場合は、71 ページの「クラスタのバックアップからの復元」へ進みます。

鍵分割資格の入力

鍵分割資格のユーザー ID とパスフレーズは、それぞれのユーザー ID とパスフレーズを所有する各個人が入力するようにしてください。この情報を 1 人が収集して入力することは、鍵分割資格を持つことの目的にそぐいません。

この時点で鍵分割資格のすべてのメンバーがこの情報を入力することが現実的でない場合は、ここでは単純な一連の資格を入力しておき、あとで OKM Manager で完全な資格を入力します。

ただし、このようにすると、セキュリティー上のリスクが生じます。単純な鍵分割資格を使用してコアセキュリティーバックアップを作成した場合は、その後バックアップの復元に使用される可能性があります。

1.「Please enter your choice:」プロンプトで、1 を入力します。次の情報が表示されます。

```
The Key Split credentials are used to wrap splits of the
Core Security Key Material which protects Data Unit Keys.

When Autonomous Unlocking is not enabled, a quorum of Key
Splits must be entered in order to unlock the KMA and allow
access to
Data Unit Keys.

A Key Split credential, consisting of a unique User Name and
Passphrase, is required for each Key Split.

The Key Split Size is the total number of splits that will
be generated.

This number must be greater than 0 and can be at most 10.


Please enter the Key Split Size: 2


The Key Split Threshold is the number of Key Splits required
to obtain a quorum.

Please enter the Key Split Threshold: 1

Please enter the Key Split User Name #1: user1

Passphrases must be at least 8 characters and at most 64
characters in length.

Passphrases must not contain the User's User Name.

Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter Key Split Passphrase #1: ********

Please re-enter Key Split Passphrase #1: ********

Press Enter to continue:

Press Ctrl-c to abort.
```

注 –
鍵分割サイズと鍵分割しきい値は、216 ページの「鍵分割設定の変更」を使用して変更できます。

鍵分割しきい値は、鍵分割サイズ以下である必要があります。

ユーザー ID とパスフレーズは、そのセキュリティーを確保するために、承認ユーザーのみが入力するようにしてください。これらの項目も、QuickStart プログラムの実行後に変更できます。

2. 「`Please enter the Key Split Size:`」プロンプトで、生成される鍵分割の数を入力して Enter キーを押します。
3. 「`Please enter the Key Split Threshold:`」プロンプトで、定足数を取得するために必要な鍵分割の数を入力して Enter キーを押します。
4. 「`Please enter the Key Split User Name #1:`」プロンプトで、最初の鍵分割ユーザーのユーザー名を入力して Enter キーを押します。
5. 「`Please enter Key Split Passphrase #1:`」プロンプトで、最初の鍵分割ユーザーのパスフレーズを入力して Enter キーを押します。
6. 「`Please re-enter Key Split Passphrase #1:`」プロンプトで、前に入力したのと同じパスフレーズを入力して Enter キーを押します。
7. 手順 4 ～手順 6 を繰り返し、選択した鍵分割サイズに対応するユーザー名とパスフレーズをすべて入力します。

注 –
鍵分割ユーザーの名前とパスフレーズは、KMA の管理のために確立されたほかのユーザーアカウントとは独立しています。

鍵分割ユーザー名は、KMA ユーザー名とは別にすることをお勧めします。

初期セキュリティー責任者ユーザー資格の入力

1. 「Press Enter to continue:」プロンプトで Enter キーを押します。次の情報が表示されます。

```
The initial Security Officer User is the first User that can
connect to the KMA via the Oracle Key Manager GUI. This User
can subsequently create additional Users and administer the
system.

Please enter a Security Officer User Name: SecOfficer

A Passphrase is used to authenticate to the KMA when a
connection is made via the Oracle Key Manager GUI.
Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User Name.

Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the Security Officer Passphrase: ********

Please re-enter the Security Officer Passphrase:
********


Press Enter to continue:
Press Ctrl-c to abort.
```

> **注 ー** セキュリティー責任者のこの初期ユーザーアカウントは、OKM Manager を使用して KMA にログオンするために使用されます。

2. プロンプトで、セキュリティー責任者のユーザー名を入力して Enter キーを押します。次の情報が表示されます。
3. プロンプトで、セキュリティー責任者のパスフレーズを入力して Enter キーを押します。
4. 「Please re-enter the Security Officer Passphrase:」プロンプトで、同じパスフレーズを再入力して Enter キーを押します。

重要 ー すべての KMA に、ユーザーやエージェントに割り当てられたパスフレーズとは独立した独自のパスフレーズが存在します。クラスタ内の最初の KMA には、ランダムなパスフレーズが割り当てられます。この KMA の証明書の期限が切れたときに、クラスタ内の別の KMA からその実体の証明書を取得する場合は、OKM Manager を使用してパスフレーズを既知の値に設定する必要があります。手順については、133 ページの「KMA のパスフレーズの設定」を参照してください。

自律ロック解除設定の指定

注意 ー 自律ロック解除を有効にすると、より便利になり、OKM クラスタの可用性が向上しますが、同時にセキュリティーリスクも発生します。自律ロック解除が使用可能である場合は、完全な起動や、格納されている鍵の復号化を行うために必要な情報が、電源が入っていない KMA に保持されている必要があります。

このため、攻撃者は盗難した KMA の電源を入れ、KMA からの鍵の抽出を開始できます。鍵の抽出は簡単ではありませんが、知識が豊富な攻撃者は KMA からすべての鍵をダンプできます。暗号化を使用した攻撃は必要ありません。

自律ロック解除が無効になっている場合は、盗まれた KMA から鍵を抽出するには暗号化を使用した攻撃が必要になります。

自律ロック解除を有効にすることを選択する前に、潜在的な攻撃やセキュリティーの問題について慎重に検討するようにしてください。

1. 「`Press Enter to continue:`」プロンプトで Enter キーを押します。次の情報が表示されます。

```
When Autonomous Unlocking is DISABLED, it is necessary to
UNLOCK the KMA using a quorum of Key Split Credentials
EACH TIME the KMA starts before normal operation of the
system can continue. Agents may NOT register Data Units
with or retrieve Data Unit Keys from a locked KMA.

When Autonomous Unlocking is ENABLED, the KMA will
automatically enter the UNLOCKED state each time the
KMA starts, allowing it to immediately service Agent
requests.

Do you wish to enable Autonomous Unlocking? [y/n]: y
```

注 ー 自律ロック解除機能を使用すると、OKM Manager を使用して定足数のパスフレーズを入力しなくても、ハードまたはソフトリセットのあとに KMA を完全な稼働状態にできます。このオプションは、あとで OKM Manager から変更できます。

2. プロンプトで、**y** または **n** を入力して Enter キーを押します。

鍵プールサイズの設定

1. 「Press Enter to continue:」プロンプトで Enter キーを押します。次の情報が表示されます。

```
Enter Key Pool Size
------------------------------------------------------------
--

Press Ctrl-c to abort.

Each KMA pre-generates and maintains a pool of keys. These
pre-operational keys must be backed up or replicated before
a KMA will provide them to an Agent for use in protecting
データ . This helps to ensure that a key will never be
permanently lost, even in disaster scenarios.

A smaller key pool size prevents unnecessary initial
database (and backup) size, but requires frequent backups
or a reliable network to ensure that activation-ready keys
are always available. Conversely, a large key pool size is
more tolerant of infrequent backups or unreliable network
connections between KMAs, but the large number of pre-
generated keys causes the database (and backups) to be
quite large.


Please select the key pool size (1000 - 200000):
```

2. プロンプトで、鍵プールサイズを入力します。入力された値によって、新しい KMA が生成して保持する初期サイズが決定されます。

KMA の時刻の同期

クラスタ内の KMA のクロックは、同期がとれている**必要があります**。内部的には、すべての KMA が UTC 時刻 (協定世界時) を使用します。

また、OKM Manager を使用して、日付と時刻の設定を現地時間に調整することもできます。

```
KMAs in a Cluster must keep their clocks synchronized.
Specify an NTP server if one is available in your network.
Otherwise, specify the date and time to which the local
clock should be set.

Please enter the NTP Server Hostname or IP Address
(optional): ntp.example.com

Press Enter to continue:
Initializing new cluster...

New cluster has been created.

Press Enter to continue:
Oracle Key Manager Version 2.5 (Build1195.1)
_____________________________________________________________
KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager
GUI in order to continue with Cluster configuration.

Press Enter to exit:

Copyright (c) 2007, 2011, Oracle and/or its futilities. All
rights reserved.
Oracle Key Manager Version 2.5 (Build1195.1)
_____________________________________________________________

Please enter your User Name:
```

1. ネットワーク環境内で NTP サーバーが使用可能な場合は、「`Please enter the NTP Server Hostname or IP Address (optional):`」プロンプトで、NTP サーバーのホスト名または IP アドレスを入力します。
2. NTP サーバーが使用可能でない場合は、Enter キーを押します。次に、「`Please enter the date and time for this KMA`」プロンプトで、指定されたいずれかの形式で日付と時刻を入力するか、または Enter キーを押して表示されている日付と時刻を使用します。
3. プロンプトで、Enter キーを押します。KMA の初期化が完了します。
4. Enter キーを押して終了します。QuickStart プログラムが終了し、ログインプロンプトが表示されます (348 ページの「KMA へのログイン」を参照)。これで、KMA に、OKM Manager と通信するために必要な最小限のシステム構成が設定されました。
5. 次の手順は、OKM Manager を使用してクラスタに接続することです。手順については、103 ページの「クラスタへの接続」を参照してください。

既存のクラスタへの参加

重要

- この作業を実行する前に、セキュリティー責任者がまず OKM Manager を使用して OKM クラスタにログインし、KMA を作成する必要があります。126 ページの「KMA の作成」を参照してください。

  KMA の初期化プロセスで指定した KMA 名 (57 ページの「KMA の初期化」を参照) が、KMA の作成時に入力した KMA 名と一致している必要があります。

- 既存の OKM クラスタに新しい KMA を追加すると、OKM クラスタは、その新しい KMA にクラスタ情報を伝播し始めます。クラスタが新しい KMA へのこれらの情報の配布を完了するには時間がかかり、結果としてこの期間中、クラスタはビジー状態になります。

  この伝播活動によって通常の操作が妨げられることのないように、クラスタへの KMA の追加は負荷の少ない時間帯に行なってください。同期期間中にエージェントが新しい KMA を使用しようとしたことによって発生する問題を回避するため、KMA は、クラスタに追加されたあともロックされた状態のままになります。KMA をロック解除する前に、その KMA が同期されるまで (つまり、クラスタ内のほかの KMA に「追い付く」まで) 待ってください。

- 以前の KMS リリースでは、新しい KMA 上で実行されているリリースがクラスタ内の既存の KMA と異なると、新しい KMA がクラスタに参加した時点で、その新しい KMA は既存の KMA のリリースに自動的にアップグレードまたはダウングレードされました。OKM 2.3 以降では、新しい KMA が OKM 2.3 以降で動作し、既存の KMA が以前の KMS リリースで動作している場合、その新しい KMA は以前のリリースにダウングレードしなくてもクラスタに参加できます。

- OKM 2.3 以降を実行している場合は、クラスタに KMA を追加する前に、複製バージョンがクラスタ内のすべての KMA によってサポートされているもっとも高い値に設定されている必要があります。229 ページの「複製バージョンの切り替え」を参照してください。

新しい KMA を既存のクラスタに加えるには、次の手順を実行します。

1. KMA の初期化プロセス (57 ページの「KMA の初期化」を参照) を完了したら、プロンプトで Enter キーを押します。

   次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can
have this KMA join an existing Cluster. You can also restore
a backup to this KMA or change the KMA Version.

Please choose one of the following:
(1)  Create New Cluster
(2)  Join Existing Cluster
(3)  Restore Cluster from Backup

Please enter your choice: 2

Join Existing Cluster
```

2. 「Please enter your choice:」プロンプトで、**2** を入力します。次の情報が表示されます。

```
Join Existing Cluster
-------------------------------------------------------------
Press Ctrl-c to abort.

In order to join a Cluster, the KMA must contact
another KMA which is already in the Cluster.

Please enter the Management Network IP Address or Host Name of an
existing KMA in the cluster: 129.80.60.172

Please enter this KMA?s Passphrase:********

Press Enter to continue:

This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1: user1

Please enter Key Split Passphrase #1: ********

Press Enter to continue:

Joining cluster...

This KMA has joined the Cluster.

Press Enter to continue:

Oracle Key Manager Version 2.3 (Build1036)
-------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager GUI
in order to continue with Cluster configuration.

Press Enter to exit:
```

注 ー この新しい KMA がクラスタ内の既存の KMA と通信できるようにするには、OKM Manager を使用して、既存の KMA のデータベース内にこの KMA のためのエントリを作成しておく必要があります。手順については、126 ページの「KMA の作成」を参照してください。

3. プロンプトで、既存のクラスタ内のいずれかの KMA のネットワークアドレスを入力して Enter キーを押します。
4. プロンプトで、その KMA のパスフレーズを入力して Enter キーを押します。
5. 最初の KMA の初期鍵分割ユーザー名を入力します。
6. 鍵分割ユーザーのパスフレーズを入力して Enter キーを押します。

重要 – 鍵分割ユーザーの名前とパスフレーズは慎重に入力してください。入力ミスがあると、この処理は失敗し、具体的な内容が示されないエラーメッセージが表示されます。攻撃者に対して公開される情報を制限するために、どの鍵分割ユーザー名またはパスフレーズが間違っているかについてのフィードバックは提供されません。

7. 手順 5 と手順 6 を繰り返し、定足数を形成するために十分な数の鍵分割ユーザーの名前とパスワードを入力します。
8. 次の「`Please enter Key Split User Name`」プロンプトで Enter キーを押します。Enter a blank name to finish.

   初期化が完了します。

   正常なクラスタ参加セッションの最後に、クラスタの複製バージョンが少なくとも 12 である場合は、QuickStart に次のプロンプトが表示されます。

```
It might take some time for this KMA to be updated with
information from other KMAs in the Cluster. This amount of
time can be greater in Clusters that have more KMAs or when
the KMAs have been online for a long time.

To accelerate these initial updates (that is, to catch up now),
you can choose now to download a backup from another KMA in
the Cluster and then restore from it. There will not be an
opportunity to accelerate these updates later.

Catch up now? [y/n]:
```

9. 初期の更新を高速化するには、**y** を入力します。それ以外の場合は、**n** を入力して手順 手順 10 に進みます。

   注 – 上のプロンプトで **y** を入力する前に、クラスタの複製バージョンを 12 に切り替えたあと、ピア KMA 上にバックアップを作成してください。また、バックアップを作成したピア KMA が現在、ネットワーク上で応答していることも確認してください。これらの手順は、新しい KMA が、ダウンロードして適用するためのキャッシュされたバックアップを見つけるのに役立ちます。

   指定した KMA は、このクラスタ内で最大のキャッシュされたバックアップを持つ別の KMA を識別し、そのバックアップをダウンロードして、それをローカルデータベースに適用します。このプロセスはデータの複製と同等ですが、それよりはるかに高速に実行されます。このプロセス中は、情報メッセージが表示されます。

次に例を示します。

```
Waiting 10 seconds for the join to propagate to Peer KMAs...

Querying Peer KMAs to find the active ones...

Querying active Peer KMAs to find cached backup sizes...

Peer KMA at IP Address 10.80.180.39 has a cached backup size of
729136 bytes.

Downloading the cached backup from this Peer KMA...

Downloaded the cached backup from this Peer KMA.

Initialized the Key Store.

Performed maintenance on the Key Store.

Applying the cached backup to the local database...

.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................

Applied the cached backup to the local database.

Successfully accelerated initial updates on this KMA.
```

あとで、新しく参加した KMA は、バックアップ内に存在しないすべてのデータを自動的に複製します。

このプロセス中にエラーが発生した場合は、QuickStart によって上のプロンプトが再度表示されます (そのエラーが一時的な状態のためである場合)。また、KMA がキャッシュされたバックアップを持つピア KMA を見つけることができない場合も、QuickStart によって上のプロンプトが再度表示されます。

ただし、上のプロンプトがはじめて表示されてから 5 分を超える時間が経過した場合は、QuickStart によって次のメッセージが表示され、上のプロンプトは表示されなくなります。

```
Failed to accelerate initial updates on this KMA after 300 seconds.
This KMA will gradually be updated with information from other
KMAs.
```

手順 9 で **y** または **n** のどちらを入力したかには関係なく、あるいはこのプロセスがタイムアウトした場合でも、次のメッセージが表示されます。

```
This KMA has joined the Cluster.

Press Enter to continue:
```

10. Enter キーを押して終了します。QuickStart プログラムが終了し、ログインプロンプトが表示されます (348 ページの「KMA へのログイン」を参照)。これで、KMA に、OKM Manager と通信するために必要な最小限のシステム構成が設定されました。
11. 次の手順は、OKM Manager を使用してクラスタに接続することです。手順については、103 ページの「クラスタへの接続」を参照してください。
12. OKM クラスタは、新しく追加された KMA に情報を伝播し始めます。これにより、新しい KMA は、クラスタ内の既存の KMA に追い付くまで非常にビジーな状態になります。ほかの KMA もまたビジーな状態になります。この動作状態は、120 ページの「KMA の表示」の説明に従って KMA を表示することによって OKM Manager から監視できます。
13. 新しい KMA の「Replication Lag Size」値を監視します。最初、この値は高くなります。「View」メニューをプルダウンして「Refresh」を選択するか、または **F5** キーを押すことによって、このパネルに表示されている情報を定期的に更新します。この KMA の「Replication Lag Size」値がクラスタ内のほかの KMA の同様の値まで下がったら、223 ページの「KMA のロック解除」の説明に従ってこの KMA をロック解除できます。

クラスタのバックアップからの復元

このオプションを使用すると、OKM Manager を使用して KMA にバックアップイメージを復元するために使用できるセキュリティー責任者アカウントを作成できます。ハードディスクの損傷など、KMA で障害が発生した場合は、バックアップを使用して KMA の構成を復元できます。ただし、出荷時のデフォルト状態に復元された KMA は既存のクラスタに簡単に参加でき、またクラスタピアから複製更新を受信することによってデータベースを構築できるため、このような操作は通常は必要ありません。それでも、KMA のバックアップからの復元は、クラスタ内のすべての KMA に障害が発生した場合に役立ちます。

注 –

最初に、バックアップを作成する必要があります。OKM Manager を使用してバックアップを作成する手順については、329 ページの「バックアップの作成」を参照してください。

最後のバックアップが実行されたときに OKM クラスタ内に存在していなかった新しいセキュリティー責任者名を指定することをお勧めします。既存のセキュリティー責任者名を指定し、別のパスフレーズを指定した場合は、古いパスフレーズが上書きされます。

既存のセキュリティー責任者名を指定し、最後のバックアップが実行される前にそのユーザーにほかの役割が追加された場合は、このユーザーにこれらのほかの役割が割り当てられなくなります。

バックアップイメージを復元するには、次の手順を実行します。

1. KMA の初期化プロセス (57 ページの「KMA の初期化」を参照) を完了したら、プロンプトで Enter キーを押します。

   次の情報が表示され、この KMA を使用して新しいクラスタを作成するか、既存のクラスタに参加するか、またはこの KMA のバックアップからクラスタを復元できることが示されます。

```
You can now use this KMA to create a new Cluster, or you can
have this KMA join an existing Cluster. You can also restore
a backup to this KMA or change the KMA Version.

Please choose one of the following:
(1)  Create New Cluster
(2)  Join Existing Cluster
(3)  Restore Cluster from Backup

Please enter your choice: 3

Restore Cluster from Backup
```

2. 「Please enter your choice:」プロンプトで、3 を入力します。次の情報が表示されます。

```
Initial Restore Cluster From Backup
Enter Initial Security Officer User Credentials
------------------------------------------------------------
Press Ctrl-c to abort.

The initial Security Officer User is the first User that
can connect to the KMA via the Oracle Key Manager GUI. This User
can subsequently create additional Users and administer
the system.

Please enter a Security Officer User ID: SO1

A Passphrase is used to authenticate to the KMA when
a connection is made via the KMS Manager.

Passphrases must be at least 8 characters and at most 64
characters in length.
```

3. プロンプトで、セキュリティー責任者のユーザー名を入力して Enter キーを押します。

ベストプラクティス : 復元の前に存在していたセキュリティー責任者ユーザー ID の代わりに、一時的な復元セキュリティー責任者ユーザー ID (たとえば、RestoreSO) を入力します。

4. プロンプトで、セキュリティー責任者のパスフレーズを入力して Enter キーを押します。

手順 5 から手順 7 は省略可能です。

QuickStart で初期の定足数ユーザー資格を定義することを選択した場合は、OKM Manager GUI からの復元操作 (手順 13) が保留されるように、この時点で定足数ログインの名前とパスフレーズを入力できます。

それにより、定足数メンバーはあとでこのログインとパスフレーズを使用して OKM Manager GUI にログインし、自分の資格を入力して復元を承認できます (201 ページの「バックアップの復元」を参照)。

ここで定足数ログインのユーザー ID を入力しない場合、QuickStart の最後に存在するユーザーは、手順 3 で作成されたセキュリティー責任者だけになります。この場合、復元を実行するには、すべての鍵分割資格を一度に入力する必要があります (手順 15)。

次の情報が表示されます。

```
Enter Initial Quorum Login User Credentials
------------------------------------------------------------

Press Ctrl-c to abort.

The initial Quorum Login User is an optional user that
will allow the restore operation to be pended until quorum
members can connect to the KMA via the Oracle Key Manager GUI and
enter their credentials. If this user is not created here,
then a quorum of credentials must be entered at the time
the restore operation is requested.

Please enter a Quorum Login User ID (optional): Q

Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User ID.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the Quorum Login Passphrase:

Please re-enter the Quorum Login Passphrase:
```

5. プロンプトで Enter キーを押すか、または定足数ログインのユーザー ID を入力して Enter キーを押します。
6. プロンプトで Enter キーを押すか、または定足数ログインのパスフレーズを入力して Enter キーを押します。
7. 「Please re-enter the Quorum Login Passphrase:」プロンプトで Enter キーを押すか、または同じパスフレーズを再入力して Enter キーを押します。

8. 「Please re-enter the Security Officer's Passphrase:」プロンプトで、手順 4 で入力したパスフレーズを再入力して Enter キーを押します。

```
Set Time Information
------------------------------------------------------------

Press Ctrl-c to abort.

KMAs in a Cluster must keep their clocks synchronized.
Specify an NTP server if one is available in your network.
Otherwise, specify the date and time to which the local clock
should be set.

Please enter the NTP Server Hostname or IP Address (optional):

The date and time for this KMA must be specified in ISO 8601 format
including a time zone. Here are some valid ISO 8601 format
patterns:

    YYYY-MM-DDThh:mm:ssZ
    YYYY-MM-DD hh:mm:ssZ
    YYYY-MM-DDThh:mm:ss-0600
    YYYY-MM-DD hh:mm:ss-0600
    YYYY-MM-DDThh:mm:ss+02:00
    YYYY-MM-DD hh:mm:ss+02:00

Please enter the date and time for this KMA [2007-09-17
22:32:53.698Z]: 2007-09-17 22:33:00-0600

Press Enter to continue:


The KMA is now ready to be restored.

Press Enter to continue:
```

9. ネットワーク環境内で NTP サーバーが使用可能な場合は、「Please enter the NTP Server Hostname or IP Address (optional):」プロンプトで、NTP サーバーのホスト名または IP アドレスを入力します。
10. NTP サーバーが使用可能でない場合は、Enter キーを押します。次に、「Please enter the date and time for this KMA」プロンプトで、指定されたいずれかの形式で日付と時刻を入力するか、または Enter キーを押して表示されている日付と時刻を使用します。

    日時が正確であることを確認します。鍵のライフサイクルは時間間隔に基づいており、鍵の元の作成時刻はバックアップに格納されます。交換用の KMA で時刻が正確に設定されていることは、意図したとおりの鍵ライフサイクルを保持するために必要不可欠です。

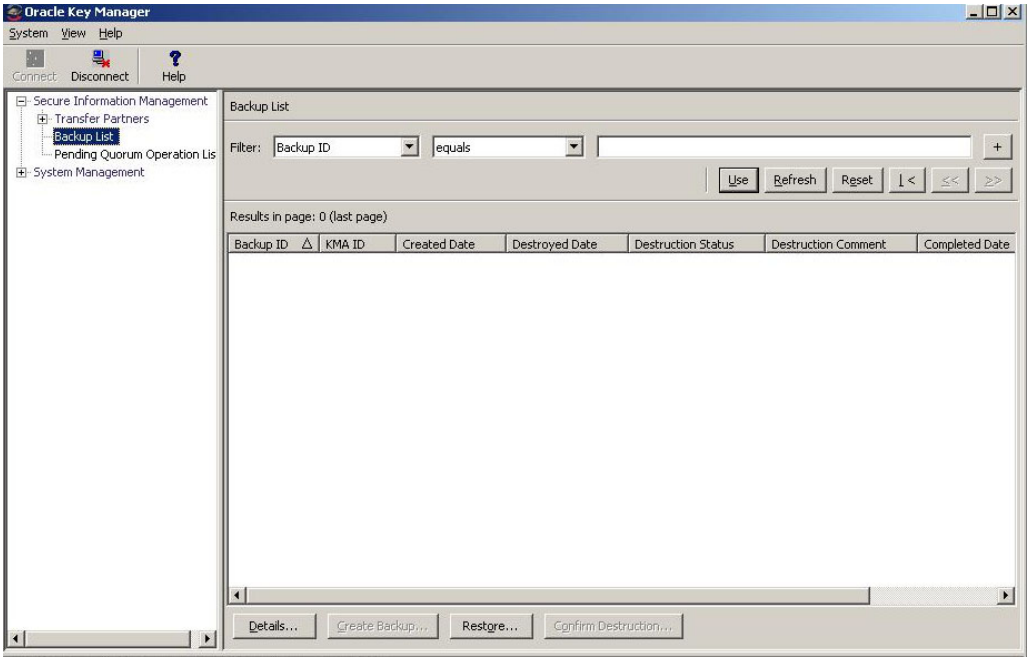
11. プロンプトで、Enter キーを押します。次の情報が表示され、初期化が完了したことが示されます。

```
Oracle Key Manager Version 2.3 (Build1036)
------------------------------------------------------------

KMA initialization complete!

You may now connect to the KMA via the Oracle Key Manager GUI
in order to continue with Cluster configuration.

Press Enter to exit:
```

12. Enter キーを押して終了します。QuickStart プログラムが終了し、ログインプロンプトが表示されます。

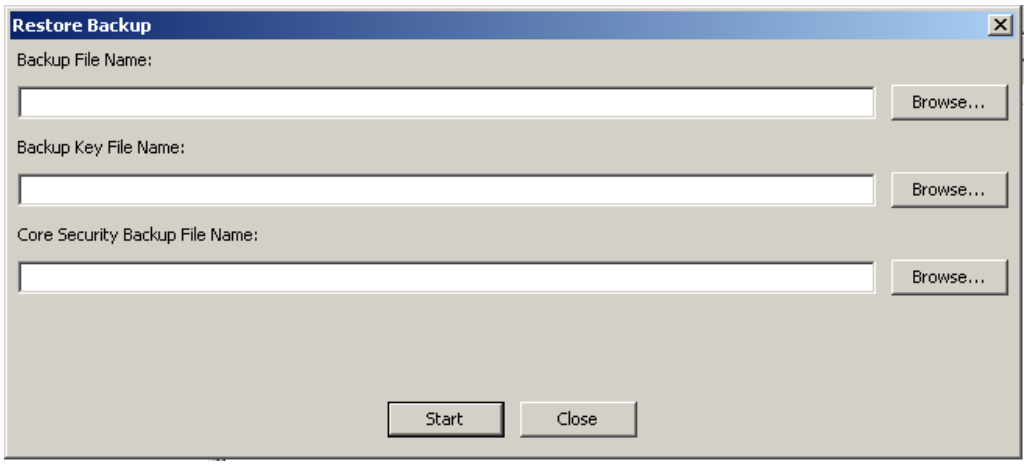
ベストプラクティス：手順 3 で確立した一時的な復元セキュリティー責任者ユーザー ID として OKM Manager GUI にログインします。

13. OKM Manager でセキュリティー責任者としてログインし、「**Backup List**」を選択します。「Backup List」画面から、「**Restore**」ボタンをクリックして、バックアップのアップロードと KMA への復元を行います。

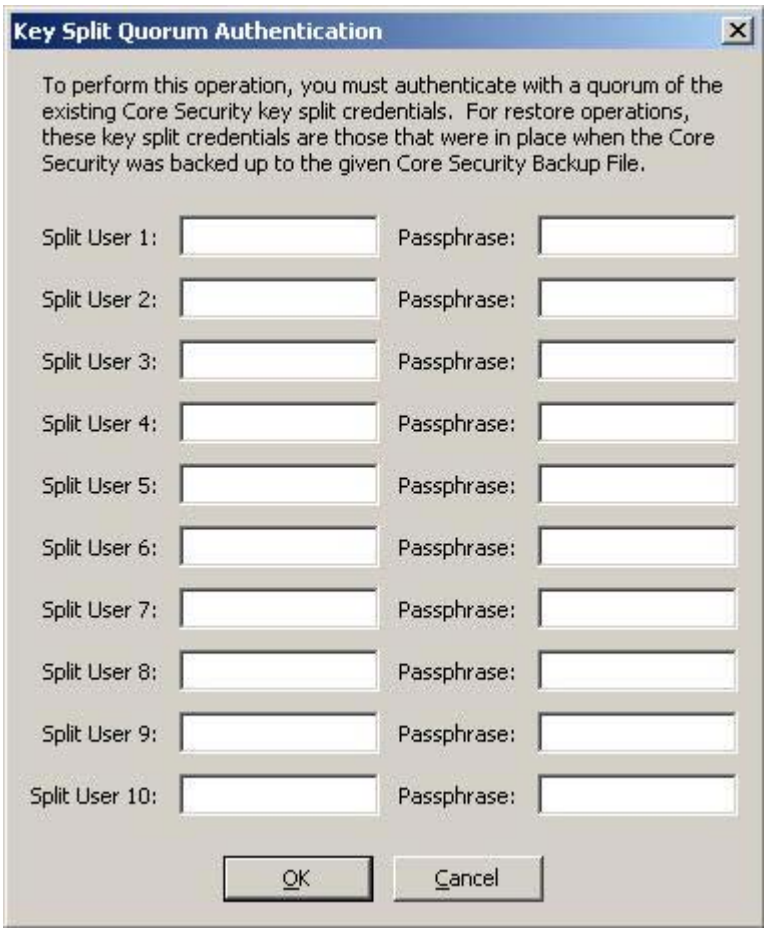


14. 復元操作を完了するために、OKM Manager から、バックアップ鍵ファイルに対応するバックアップファイル、バックアップ鍵ファイル、およびコアセキュリティーバックアップファイルの入力が求められます。

    バックアップ鍵ファイルとバックアップファイルは一致している必要がありますが、コアセキュリティーバックアップファイルは任意のものを使用できます。



15. 次に、OKM Manager から定足数の鍵分割ユーザーの入力が求められます。このユーザーは、コアセキュリティーバックアップが実行されたときに有効だった鍵分割資格ユーザーである必要があります。



復元が完了すると、バックアップ (コアセキュリティーバックアップではない) の完了時に有効だった鍵分割資格が復元されます。

重要 – 鍵分割ユーザーの名前とパスフレーズは慎重に入力してください。入力ミスがあると、この処理は失敗し、具体的な内容が示されないエラーメッセージが表示されます。攻撃者に対して公開される情報を制限するために、どの鍵分割ユーザー名またはパスフレーズが間違っているかについてのフィードバックは提供されません。

16. 復元処理が完了すると、新しいクラスタが作成されます。

ベストプラクティス : クリーンアップの手順として、元の (復元の前に存在していた) セキュリティー責任者ユーザー ID を使用して OKM Manager GUI にログインし、一時的な復元セキュリティー責任者ユーザー ID を削除します。147 ページの「ユーザーの削除」を参照してください。

エージェントの追加およびテープドライブの登録

KMA を設定したあと、エージェントを追加したり、その KMA を使用するテープドライブを登録したりすることができます。

1. オペレータとして OKM Manager GUI にログインし、エージェントを作成します (299 ページの「エージェントの作成」を参照)。
2. VOP (Virtual Operator Panel) を使用して、次の操作を実行します。VOP への接続方法やその使用方法がわからない場合は、VOP のマニュアルを参照してください。
   a. サービス担当者にテープドライブのライセンスの取得を依頼します (『OKM Installation and Service Manual』の第 3 章にある「License the Tape Drives」を参照)。この機能を実行するには、VOP (Virtual Operator Panel) を使用します。
   b. サービス担当者からのガイダンスを使用して、テープドライブを登録します (『OKM Installation and Service Manual』の第 3 章にある「Enroll the Tape Drives」を参照)。

      次の情報を指定する必要があります。

      - このドライブで永続的暗号化テープドライブを使用するかどうか。
      - この機器のエージェント ID、パスフレーズ、および OKM IP アドレス。
3. コンプライアンス責任者として OKM Manager GUI にログインし、少なくとも 1 つの鍵グループを作成して (256 ページの「鍵グループの作成」を参照)、この鍵グループにテープドライブ (エージェント) を割り当てます (268 ページの「エージェントへの鍵グループの割り当て」および『OKM Installation and Service Manual』にある「Enroll the Tape Drives」を参照)。

   この鍵グループをデフォルトとして割り当てる必要があります。そうしないと、このドライブでの書き込みができません。デフォルトを指定しない場合、このドライブは、割り当てられたグループに対して読み取り専用になります。

3

OKM Manager の使用

この章では、OKM Manager と次の手順について説明します。

- OKM Manager ソフトウェアのインストール (80 ページ)
- OKM Manager の起動 (87 ページ)
- OKM Manager ソフトウェアのアンインストール (101 ページ)

また、メニューと区画についても簡単に説明します。

OKM Manager について

OKM Manager は、KMA のクライアントとして機能するアプリケーションです。KMS Manager は、KMA の設定、制御、および監視に使用できます。ユーザーは、割り当てられている役割に応じて、さまざまな操作を実行できます。

OKM Manager ソフトウェアのインストール

OKM Manager ソフトウェアのインストーラをダウンロードするには、次の手順を実行します。

1. 次の場所にある My Oracle Support (MOS) Web サイトにログインします。

   https://support.oracle.com/

2. 「Patches & Updates」タブ (ウィンドウの上端の近くにあります) を開きます。
3. 「Patch Search」区画で、「Search」タブが開いた状態で、「**Product or Family (Advanced)**」をクリックします。
4. 「**Include all products in a family**」のボックスにチェックマークを付けます。
5. 「Product」フィールドに **OKM** または **key** を入力し、プルダウンリストから「Oracle Key Manager (OKM)」を選択します。
6. 「Release」フィールドドロップダウンで、「**Oracle Key Manager (OKM) 2.4**」を選択します。
7. 「Release」ドロップダウンウィンドウを閉じ、「**Search**」ボタンをクリックします。

OKM のインストールの開始

重要 ー 新しい OKM Manager をインストールする前に、OKM Manager の以前のバージョンをすべてアンインストールしてください。

1. Windows または Solaris システムのどちらを実行しているかに応じて、インストールプログラムを起動するための適切なプロセスを選択します。

- Windows の場合は、インストールプログラムを起動するためのショートカットをダブルクリックします。
- Solaris の場合は、次の手順を実行します。

  a. DISPLAY 環境を、このインストーラが表示されるシステムを識別するように設定します。

     i. インストールプログラムをローカルの Solaris システムで起動する場合は、DISPLAY 環境変数を「:0.0」に設定します。

     ii. インストーラをダウンロードしたディレクトリに移動します。

     iii. インストーラを起動します。

     たとえば、インストーラを /tmp ディレクトリにダウンロードし、それをローカルの Solaris システムで起動しようとしている場合は、シェルプロンプトで次のコマンドを入力することによってインストーラを起動します。

```
DISPLAY=:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

注 ー ある Solaris システムでインストーラを起動し、そのインストーラを別の Solaris システムで表示されるようにする場合は、それが表示されるシステムを識別するように DISPLAY 環境変数を設定します。表示システムで、最初に xhost (1) ユーティリティーを実行して、インストーラを起動するシステムからのアクセスを許可します。

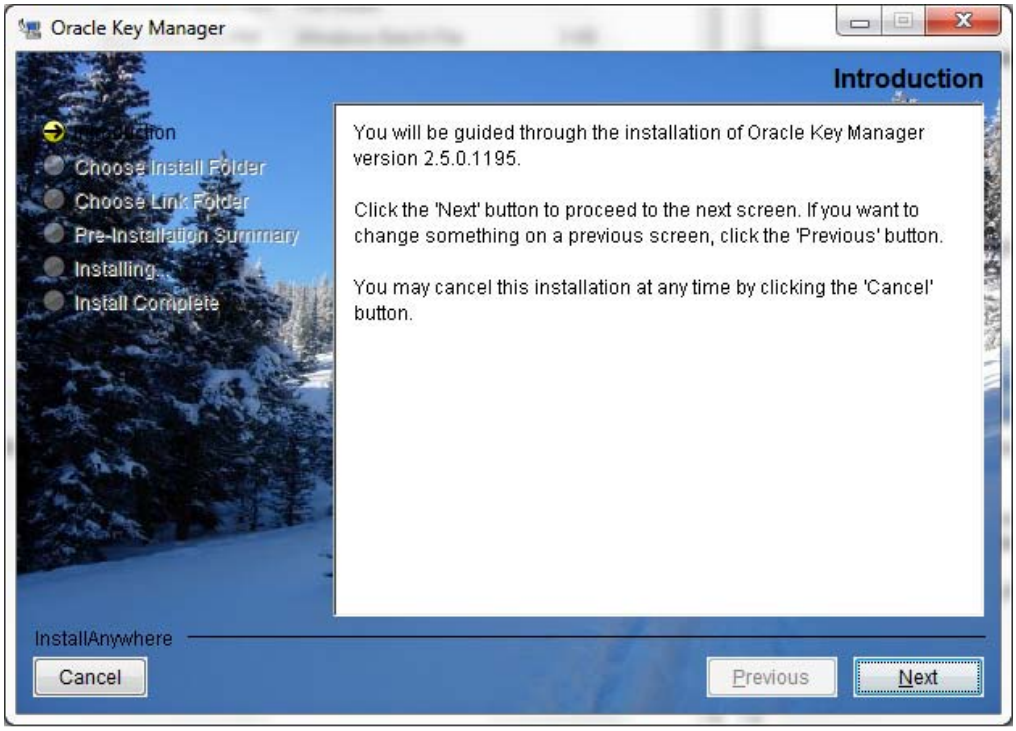
たとえば、インストーラを表示する (「hosta」という名前の) システムで、次のように入力します。

xhost +

インストーラを起動するシステムでは、次のように入力します。

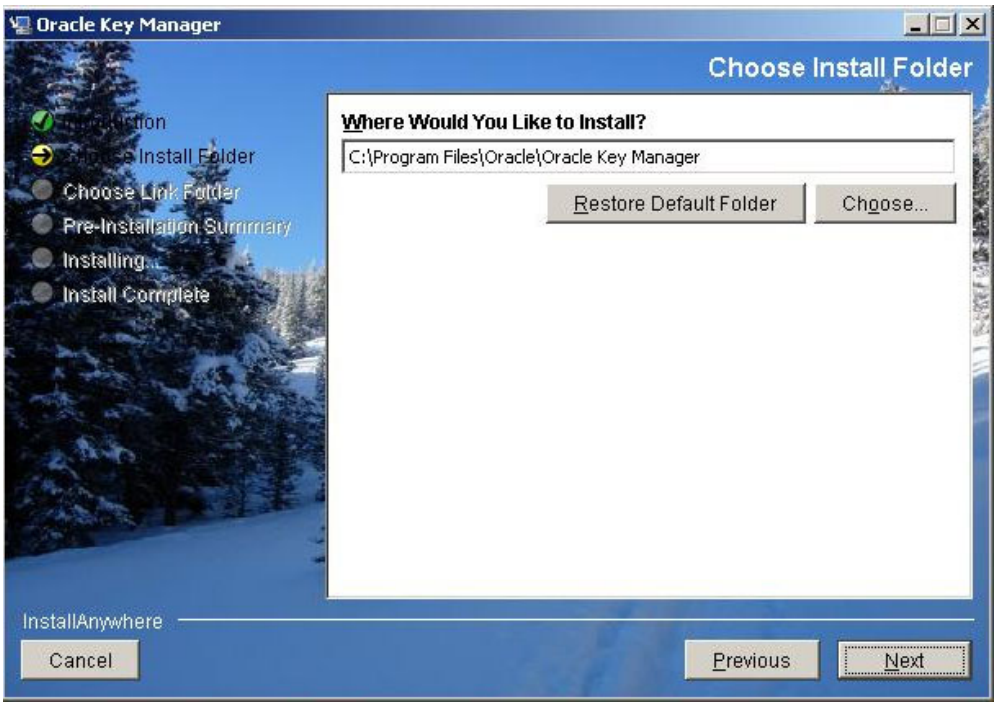
```
ping hosta
DISPLAY=hosta:0.0
export DISPLAY
cd /tmp
ls install.bin
sh ./install.bin
```

「Introduction」ウィンドウが表示されます。次の画面例は、Windows システムの場合です。



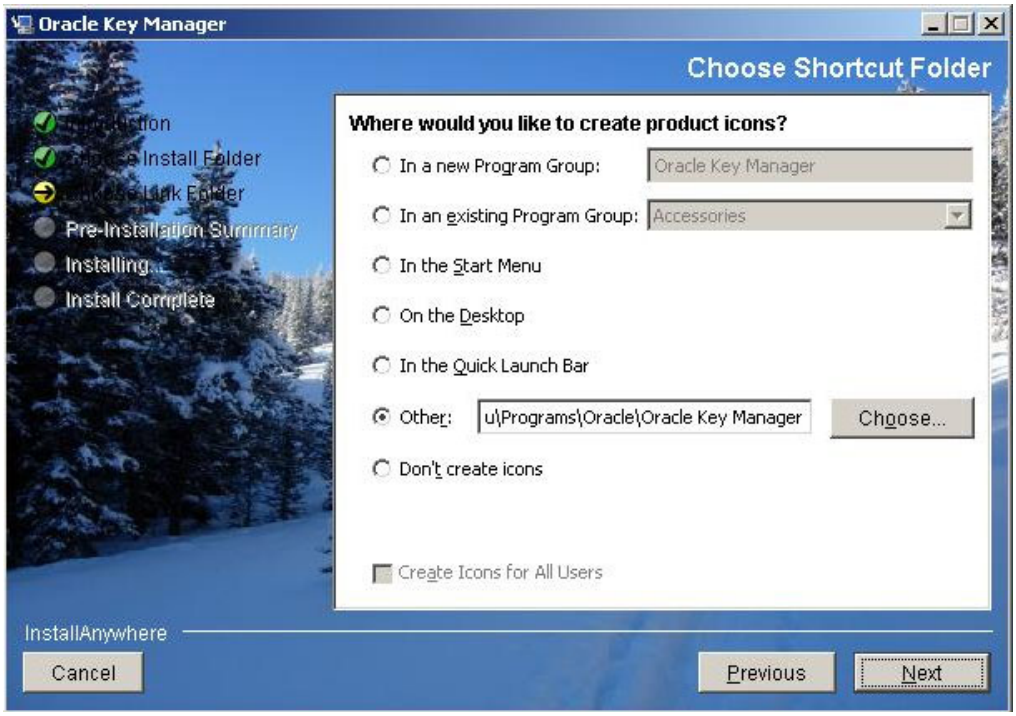
2. 「Next」を選択します。

3. 「Choose Install Folder」ウィンドウが表示されます。



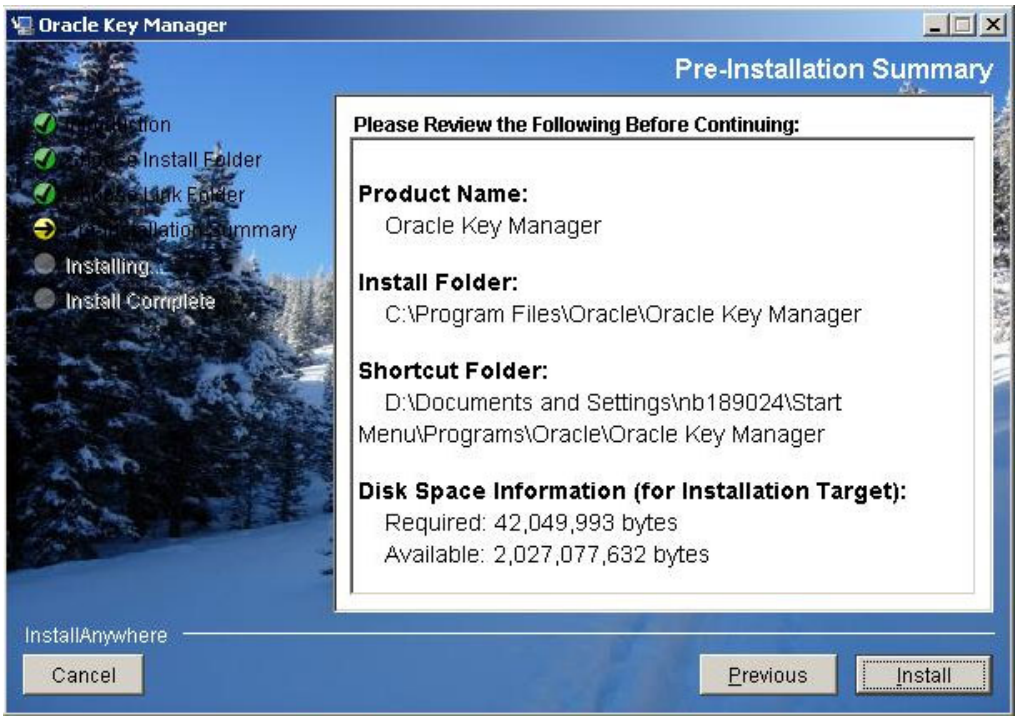
4. そのまま「Next」をクリックしてデフォルトのフォルダを選択するか、または独自のインストールフォルダを指定して「Next」をクリックします。

5. 「Choose Shortcut Folder」ウィンドウが表示されます。ここでは、必要な場所に製品アイコンを作成できます。

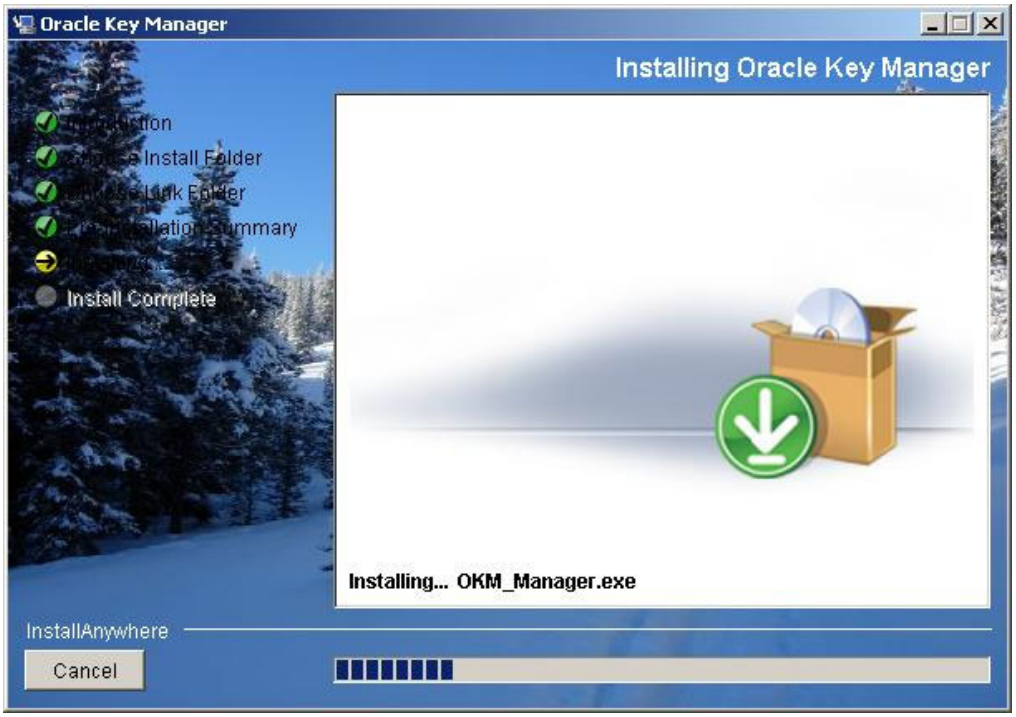


6. 選択してから「Next」をクリックします。

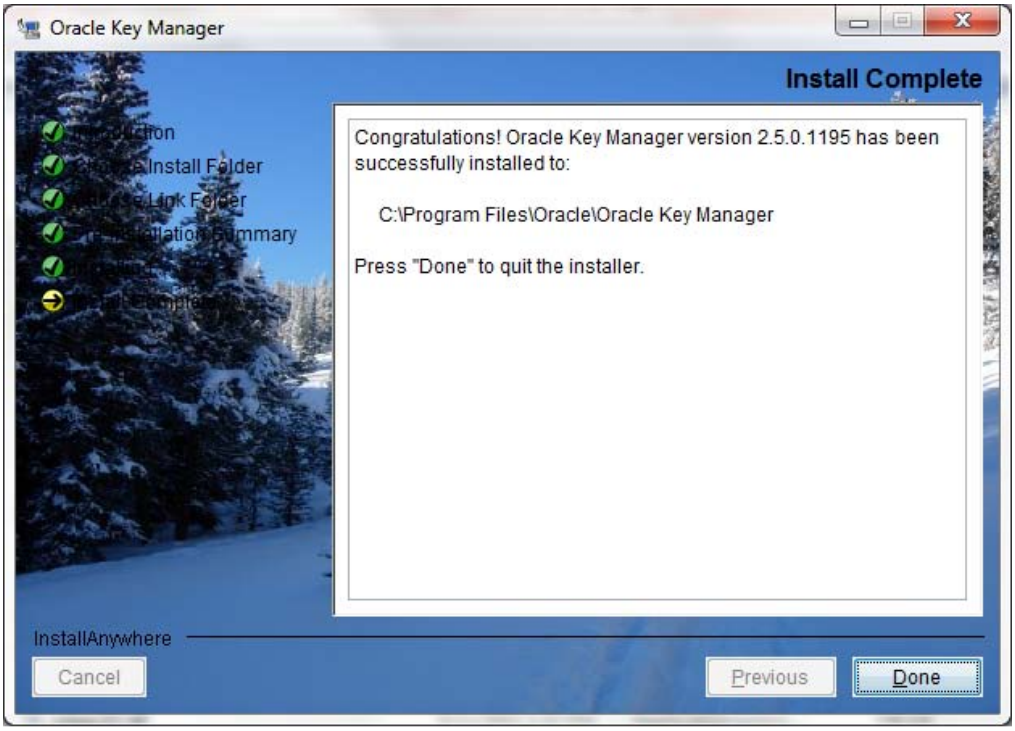
7. 「Pre-Installation summary」画面が表示されます。



8. 「Install」を選択して OKM Manager をインストールするか、または「Previous」を選択して設定を変更します。



9. これで、イントール処理は完了です。「Done」を選択して終了します。



OKM Manager の起動

OKM Manager を起動するには、環境に応じて次の 2 つの方法のどちらかを使用できます。

- Windows での起動
- Solaris での起動

Windows での OKM Manager の起動

インストールプログラムでショートカットを作成するように指定した場合は、そのショートカットをダブルクリックして OKM Manager アプリケーションを起動します。

それ以外の場合は、Windows エクスプローラを起動し、OKM Manager をインストールした場所に移動して OKM_Manager.exe を起動します。

Solaris での OKM Manager の起動

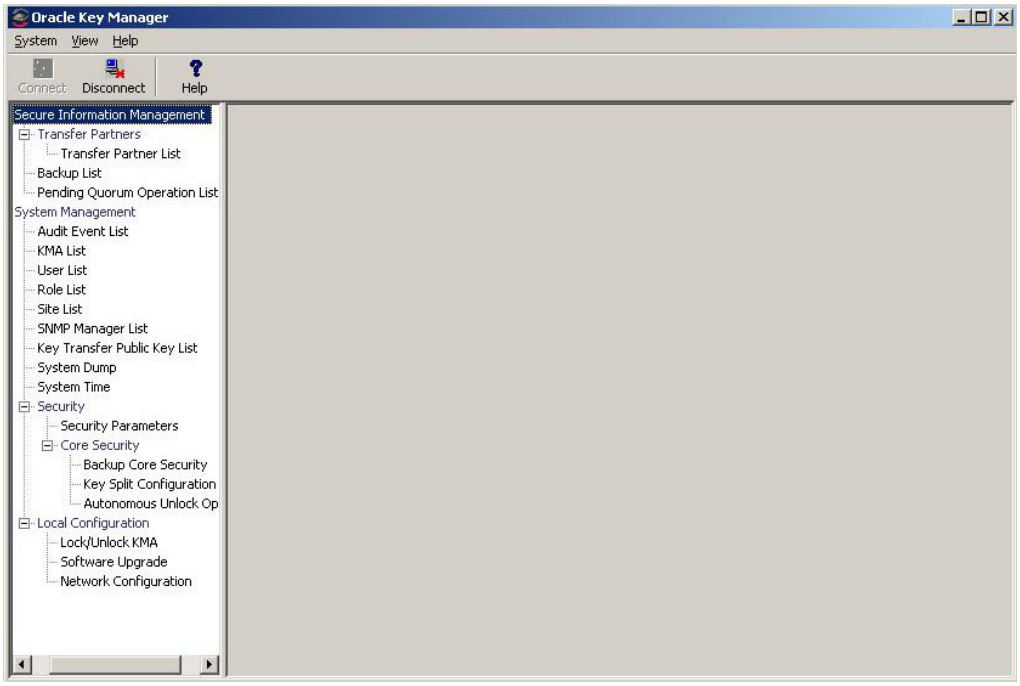
Windows の場合と同様に、インストールプログラムでショートカットを作成するように指定できます。たとえば、ホームディレクトリにショートカットを作成した場合は、シェルプロンプトで次のように入力して起動することができます。

```
~/OKM_Manager
```

あるいは、OKM Manager をインストールした場所に移動して OKM_Manager exe を起動することもできます。

OKM Manager GUI の概要

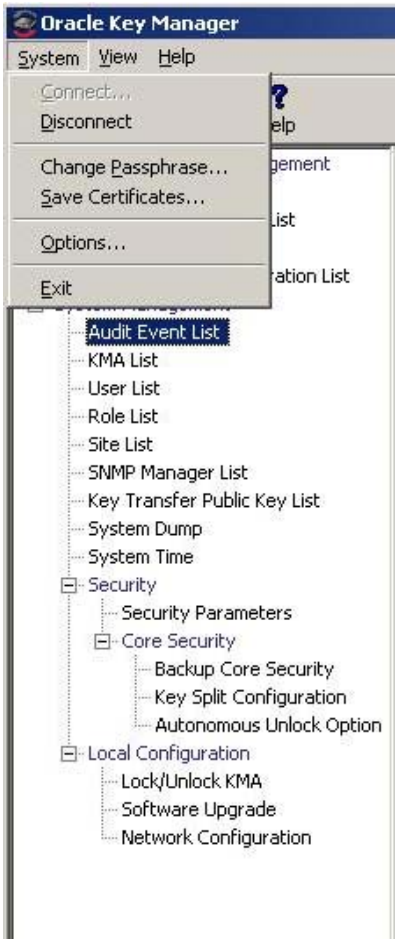
OKM Manager GUI を、サンプルのメニューとともに次に示します。



OKM Manager GUI には、「System」メニュー、「View」メニュー、および「Help」メニューが含まれています。該当するアクションバー項目をクリックしてメニューを表示してから、メニュー項目を選択します。

ツールバーのボタンは、いくつかのメニューオプションへのショートカットを提供します。

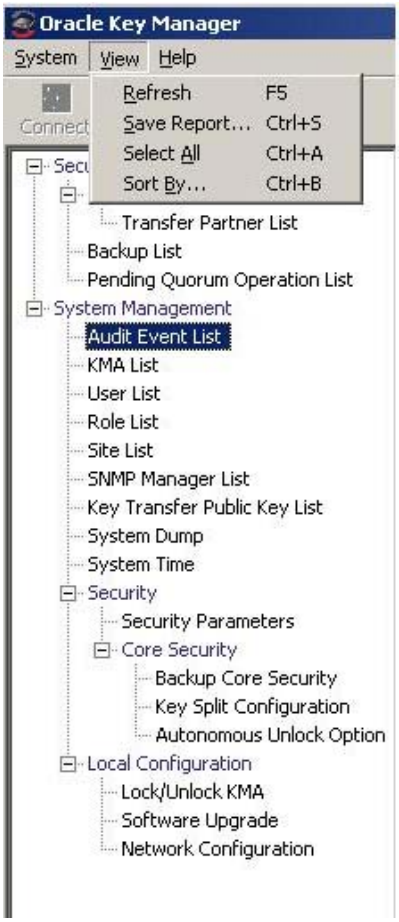
「System」メニュー



「System」メニューのオプション

- 「**Connect**」**:** プロファイルを使用して既存のクラスタに接続したり、新しいクラスタプロファイルを作成したりできる「Connect to Cluster」ダイアログボックスを表示します。
- 「**Disconnect**」**:** KMA からユーザーを切り離す「Disconnect from KMA」ダイアログボックスを表示します。
- 「**Change passphrase**」**:** パスフレーズを変更できる「Change passphrase」ダイアログボックスを表示します。
- 「**Save Certificates**」**:** CA 証明書やクライアント証明書のファイル名を編集できる「Save Certificates」ダイアログボックスを表示します。
- 「**Options**」**:** 各種の設定を指定するために使用される「Options」ダイアログボックスを表示します。
- 「**Exit**」**:** OKM Manager GUI を終了します。

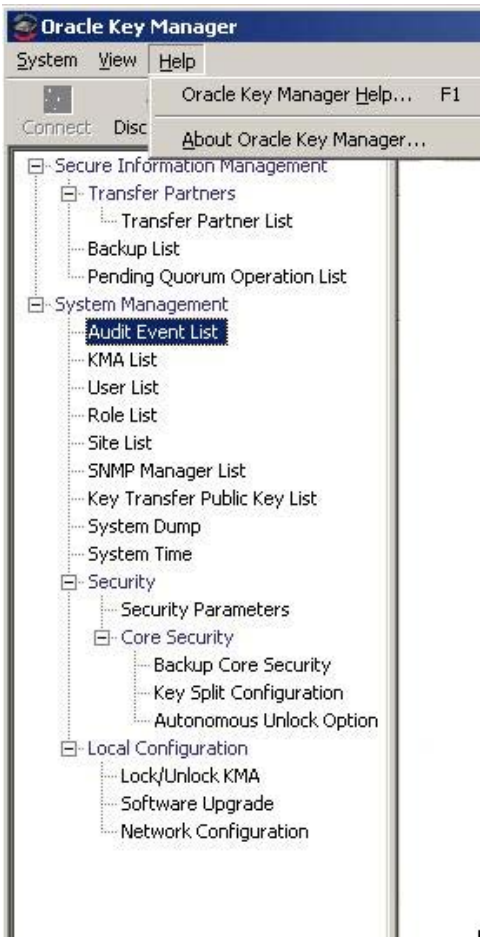
「View」メニュー



「View」メニューのオプション

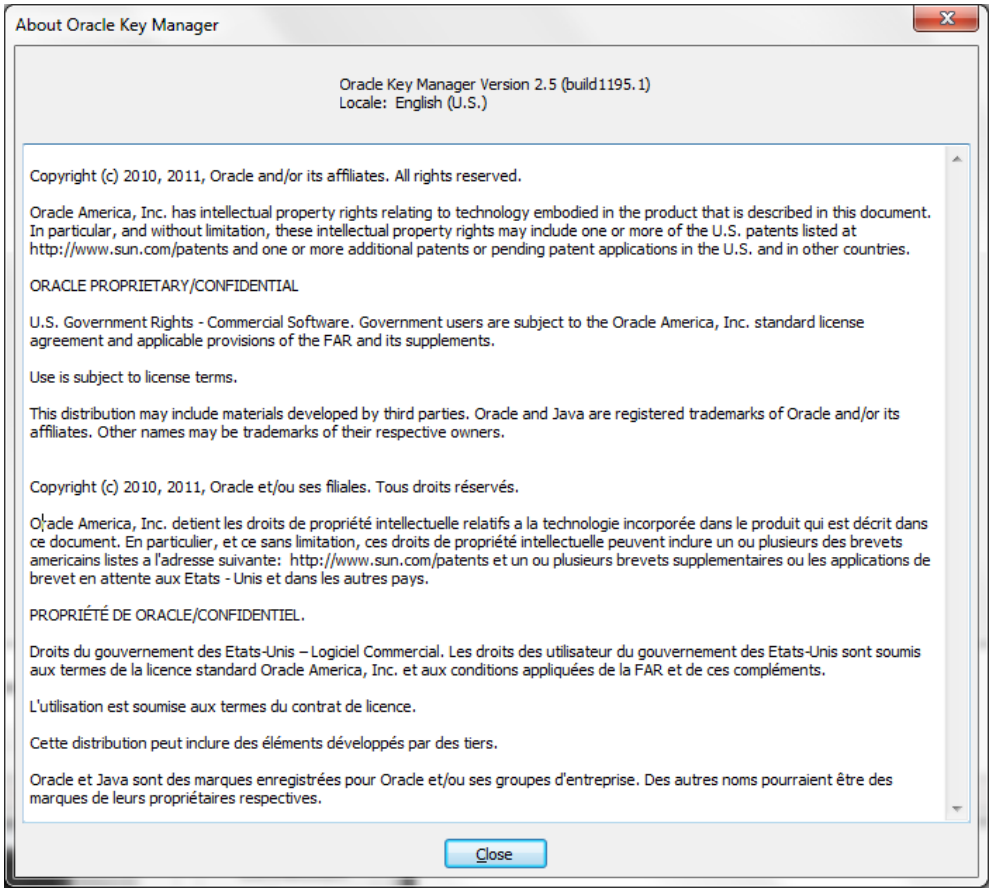
- **Refresh:** 画面を再表示します。
- **「Save Report」:**「Save Report」を使用すると、任意のリスト画面の内容を OKM Manager が実行されているシステム上のテキストファイルにダウンロードできます。
- **Select All:**「Select All」を選択すると、「List」画面上のすべての項目が選択されます。
- **Sort By:**「List」画面上の項目のリストをソートします。これは、リストの列見出しをクリックすることと同じです。

「Help」メニュー


Oracle Key Manager
System
View
Help
Oracle Key Manager Help... F1
About Oracle Key Manager...
Connect
Disc
Secure Information Management
Transfer Partners
Transfer Partner List
Backup List
Pending Quorum Operation List
System Management
Audit Event List
KMA List
User List
Role List
Site List
SNMP Manager List
Key Transfer Public Key List
System Dump
System Time
Security
Security Parameters
Core Security
Backup Core Security
Key Split Configuration
Autonomous Unlock Option
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration

「Help」メニューのオプション

- 「**OKM Manager Help**」**:** OKM Manager のオンラインヘルプの索引と目次を表示します。
- 「**About OKM Manager**」**:** OKM Manager のバージョン情報と著作権情報を表示します。このダイアログボックスを閉じるには、「Close」ボタンをクリックします。



ツールバーのボタン

次の表に、OKM のツールバーボタンの説明を示します。

ボタン	説明
	プロファイルを選択することによって KMA に接続できる「Connect to KMA」ダイアログボックスを表示します。
	KMA から切り離すことのできる「Disconnect from KMA」ダイアログボックスを表示します。
	OKM のオンラインヘルプの索引と目次を表示します。

ショートカットキー

ショートカットキーを使用すると、複数のコマンドを 1 回の操作で選択できます。次のショートカットキーが使用されています。

現在の選択の切り取り	Ctrl+X
現在の選択のコピー	Ctrl+C
クリップボードの内容を現在の選択ポイントにコピー	Ctrl+V
レポートをローカルサイトに保存するためのダイアログボックスの表示	Ctrl+S

メニューアクセラレータキー

すべてのメニュー項目について、メニューアクセラレータキーがサポートされています。アクセラレータキーを表示するには、Alt キーを押したままにします。

オンラインヘルプの使用法

オンラインヘルプを使用すると、OKM に関する詳細な情報を表示できます。オンラインヘルプの使用は簡単です。トピックはさまざまな方法で表示できます。次の操作を行うことができます。

- 目次の参照
- キーワードの検索
- 索引の使用
- 前に表示したページへの移動
- トピックの印刷

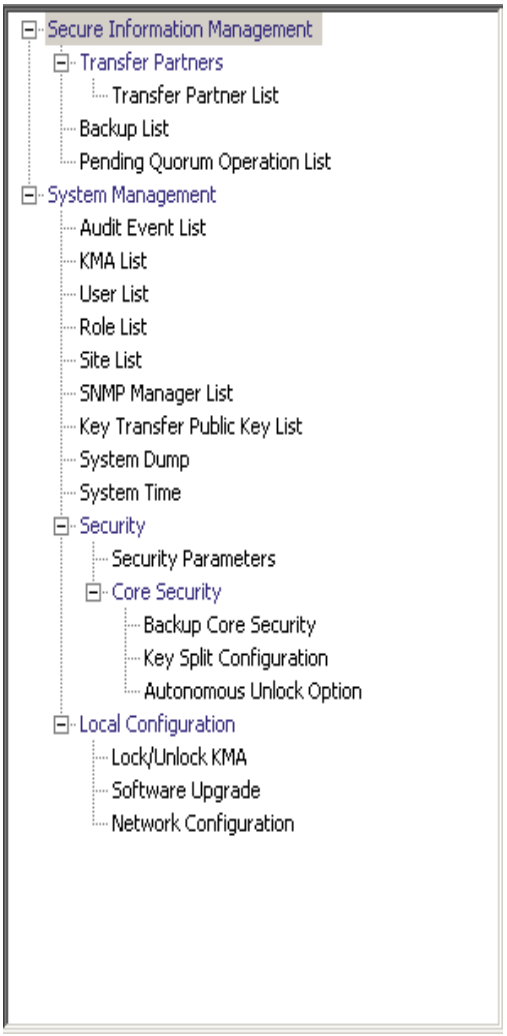
OKM Manager GUI の区画

OKM Manager GUI には、次の 3 つの区画が含まれています。

- OKM 管理操作ツリー
- OKM 管理操作の詳細
- セッション監査ログ

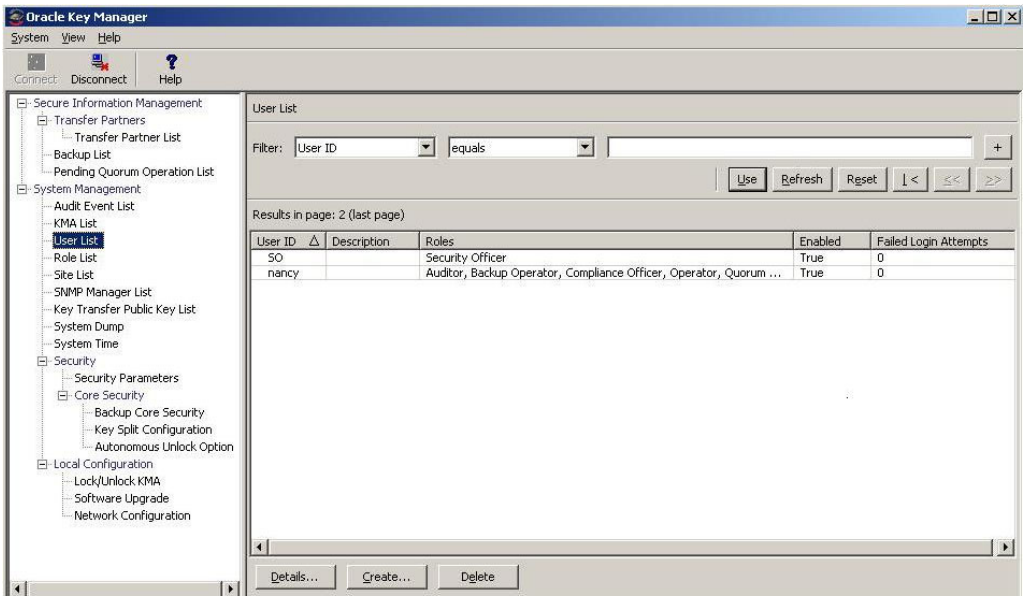
OKM 管理操作ツリー区画

画面の左側に配置されている OKM 管理操作ツリー区画には、OKM のすべての操作機能が表示されます。このツリー区画に表示されるオプションは、割り当てられている役割に応じて異なります。次の例では、セキュリティー責任者が実行できる操作が表示されています。



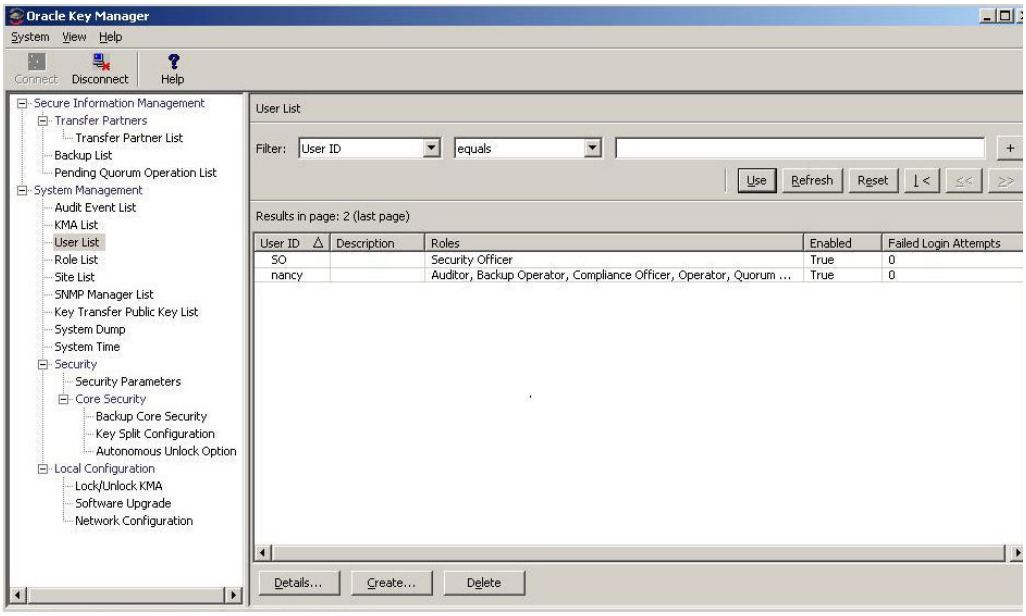
OKM 管理操作の詳細区画

ある操作が選択されると、操作ツリー区画の右にある OKM Manager 操作の詳細区画には、選択された操作に必要なコンポーネントが表示されます。各リストパネルに表示される項目に対してフィルタを適用できます。次に、操作ツリー区画で「System Management」メニューの「User List」メニューオプションを選択した場合の「User List」の例を示します。



セッション監査ログ区画

操作ツリー区画と操作の詳細区画の下がセッション監査ログ区画です。ここには、最近のセッションイベントのスクロール可能なリストが表示されます。

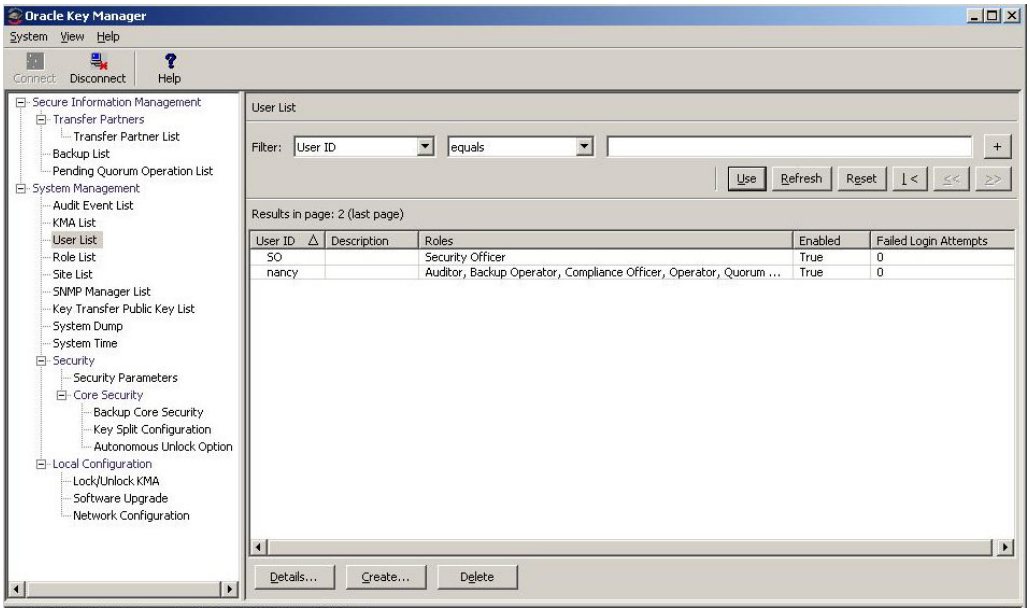


ステータスバー

画面最下部にあるステータスバーは、次のフィールドで構成されています。

- 「**User Name**」**:** 現在ログインしているユーザーのユーザー名を表示します。次に示す画面では、セキュリティー責任者 (SO) がログインしています。
- 「**Connection Status**」**:** 現在の接続の状態 (つまり、「Connected」) を表示します。
- **KMA IP アドレス :** 管理ネットワーク IP アドレスとターゲット KMA の名前が表示されます。

KMA に接続していない場合、状態フィールドは空白になります。



パネル

OKM Manager の各画面には、共通のパネルコンポーネントがあります。ここでは、各コンポーネントについて説明します。

タイトル

画面のタイトルが表示されます。

フィルタ

特定のキーを使用してデータベースをフィルタできます。次のコンポーネントが含まれます。

テーブルラベル : フィルタ処理を適用するテーブルを指定します。

フィルタ属性コンボボックス : フィルタ処理の対象となるフィールドを示します。

フィルタ演算子 1 コンボボックス : フィルタ値 1 に適用されるフィルタ演算子を指定します。フィルタ演算子は、次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 コントロール : 単一の値として使用されるか、またはフィルタキーの範囲の開始値として使用されます。

フィルタ値 2 コントロール : 単一の値として使用されるか、またはフィルタキーの範囲の終了値として使用されます。

「Use」ボタン : 表示されているリストにフィルタを適用します。

更新 :

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

> **注 ー** 出力されるレコードの数が「Query Page Size」より大きい場合は、複数のページが表示されます。フィルタの下の各ボタンをクリックすると、ページ間を移動できます。

ソート :

列見出しをクリックすると、リストがそのフィールドでソートされます。出力に複数のページが必要である場合は、結果の全体がソートされてから、対応するページが返されます。

メッセージ

データベースクエリーに関連するメッセージが表示されます。これは、「Database View」リストと連動して動作します。次のコンポーネントが含まれます。

- 静的テキストラベル : 次のようなエラーメッセージが表示されます。

  ```
  Result limit exceeded. 10,000 results returned. Use a filter
  to reduce the filter size.
  ```

OKM Manager ソフトウェアのアンインストール

OKM ソフトウェアのアンインストールを開始するには、次の 2 つのオプションを使用できます。

- アンインストールプログラムが存在するディレクトリに移動し、そこから実行可能ファイルを起動します。
- Windows ユーザーの場合のみ、「プログラムの追加と削除」プロセスを起動します。

どちらの場合でも、これらの手順を完了したあとに「Preparing Setup」ウィンドウが表示されます。102 ページの「アンインストール処理の完了」を参照してください。

実行可能ファイルの起動

OKM Manager ソフトウェアをアンインストールするには、次の手順を実行します。

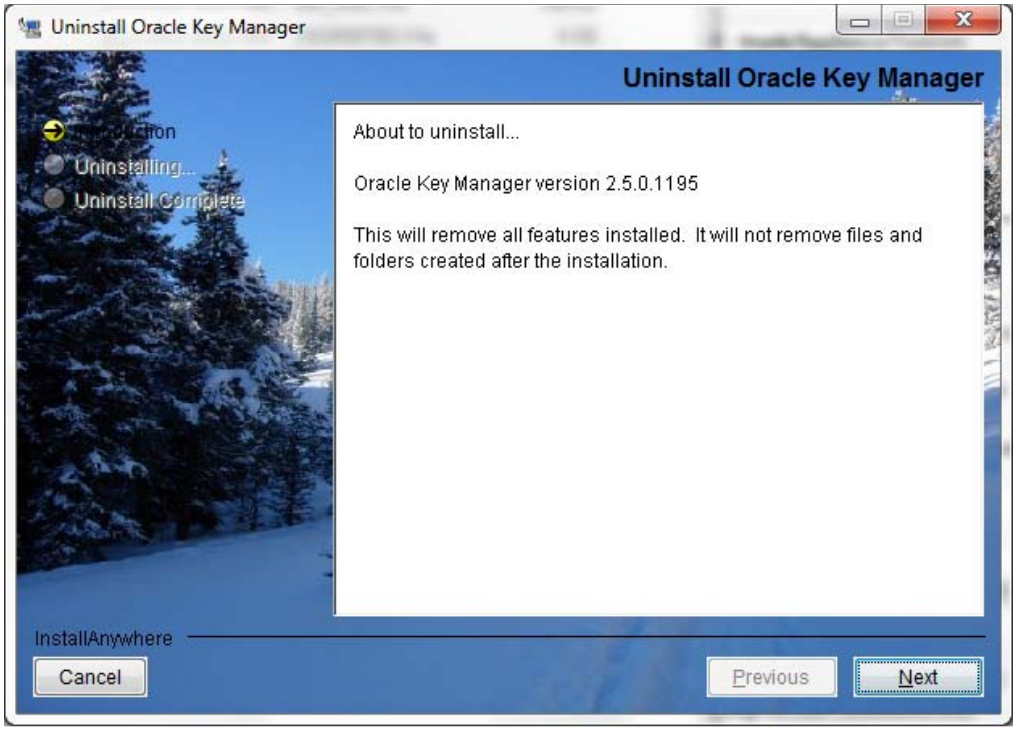
1. OKM Manager がインストールされたディレクトリの下にある「Uninstall_Oracle_Key_Manager」ディレクトリに移動します。
2. 「Uninstall_Oracle_Key_Manager.exe」(Windows) または「Uninstall_Oracle_Key_Manager」(Solaris) 実行可能ファイルを起動して、アンインストールプロセスを起動します。
3. インストールおよびアンインストールプログラムによってアンインストール処理の準備が行われる間、「Preparing Setup」ウィンドウが表示されています。

「プログラムの追加と削除」の起動 (Windows のみ)

1. 「**スタート**」をクリックし、「**設定**」、「**コントロールパネル**」の順に選択して、「**プログラムの追加と削除**」をダブルクリックします。「プログラムの追加と削除」ウィンドウが表示されます。リストをスクロールダウンし (ソフトウェアが表示されていない場合)、「Sun KMS Manager」を選択して、「変更と削除」ボタンをクリックします。
2. インストールおよびアンインストールプログラムによってアンインストール処理の準備が行われる間、「Preparing Setup」ウィンドウが表示されています。

アンインストール処理の完了

「OKM uninstall」ダイアログボックスが表示され、選択されたアプリケーションとそのすべての機能を削除することを確認するよう求められます。



1. 「Next」ボタンをクリックして続行するか、または「Cancel」ボタンをクリックしてプロセスを停止し、「プログラムの追加と削除」ウィンドウ (Windows) またはシェルプロンプト (Solaris) に戻ります。

   注 ー 接続プロファイルは削除されません。

2. アンインストール処理が完了すると、「Uninstall Complete」ウィンドウが表示されます。このウィンドウを閉じるには、「Finish」ボタンをクリックします。このウィンドウを閉じて、「プログラムの追加と削除」ウィンドウ (Windows) またはシェルプロンプト (Solaris) に戻ります。

4

「System」メニューの使用法

この章では、OKM Manager を使用して KMA に接続するための詳細な手順について説明します。また、「System」メニューのその他のオプションを使用する手順についても説明します。

クラスタへの接続

重要 – KMA に接続する前に、少なくとも 1 つのクラスタプロファイルが存在する必要があり、さらに KMA 上でユーザーが作成され、有効になっている必要があります。

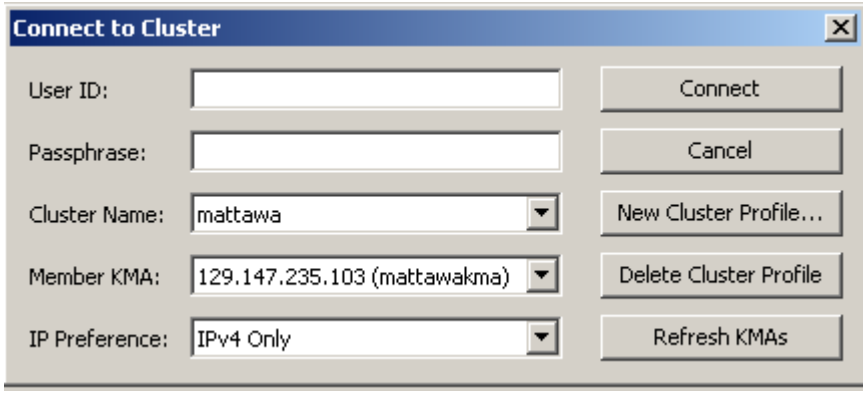
この節では、OKM Manager を使用して KMA に接続するための手順について説明します。はじめて KMA に接続する場合は、最初にクラスタプロファイルを定義する必要があります。それ以降は、作成したクラスタプロファイルを使用して KMA に接続できます。OKM Manager は、クラスタプロファイル情報を使用して、クラスタ (KMA IP アドレス) との通信を開始します。

クラスタプロファイルの作成

クラスタプロファイルを作成するには、次の手順を実行します。

1. 「System」メニューから「**Connect**」を選択するかまたは、ツールバーの 

をクリックします。「Connect to Cluster」ダイアログボックスが表示されます。既存のプロファイルが存在する場合は、クラスタプロファイルの名前と IP アドレスがそれぞれ、「Cluster Name」フィールドと「IP Address」フィールドに表示されます。



2. 「**New Cluster Profile**」ボタンをクリックします。「Create Cluster Profile」ダイアログボックスが表示されます。

3. 次のパラメータを設定します。

クラスター名

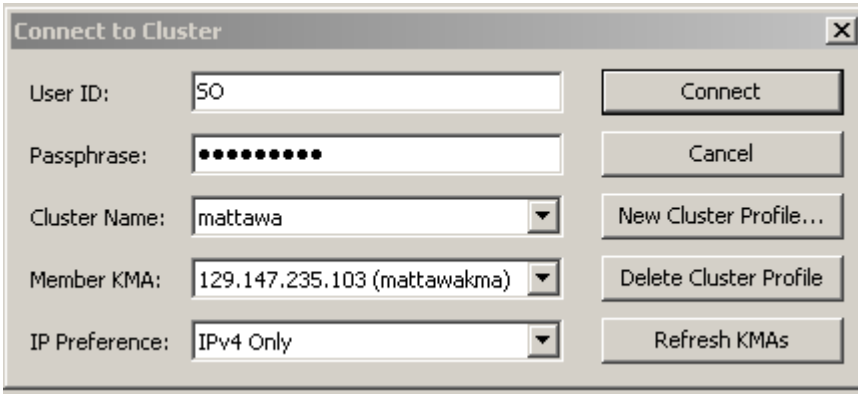
クラスタプロファイル名を一意に識別する値を入力します。

Initial IP Address or Host Name

接続先となる、このクラスタ内の最初の KMA のサービスネットワーク IP アドレスまたはホスト名を入力します。接続先のネットワークの選択は、OKM Manager が実行されているコンピュータシステムの接続先のネットワークによって決まります。

> **注 ー** クラスタプロファイルは、クラスタ全体を対象としており、エージェントのすべてのユーザーがこれを使用できるため、1 つ作成するだけで済みます。別のクラスタプロファイルの作成が必要になるのは、2 番目のクラスタを確立したい場合か、または現在のクラスタ内のすべての KMA の IP アドレスを変更した場合のみです。

4. 「**OK**」ボタンをクリックします。「Connect to Cluster」ダイアログボックスが表示され、作成したクラスタプロファイルの情報が示されます。



5. 次のパラメータを入力し、「**Connect**」ボタンをクリックします。

ユーザー ID

指定された KMA に接続するユーザーの名前を入力するか、または最初の QuickStart 処理を実行したあとにはじめて KMA に接続する場合は、QuickStart の処理中に作成されたセキュリティー責任者の名前を入力します。

パスフレーズ

選択したユーザーのパスフレーズを入力します。

クラスター名

接続先のクラスタを選択します。

Member KMAs

このクラスタ内の接続先となる KMA を選択します。

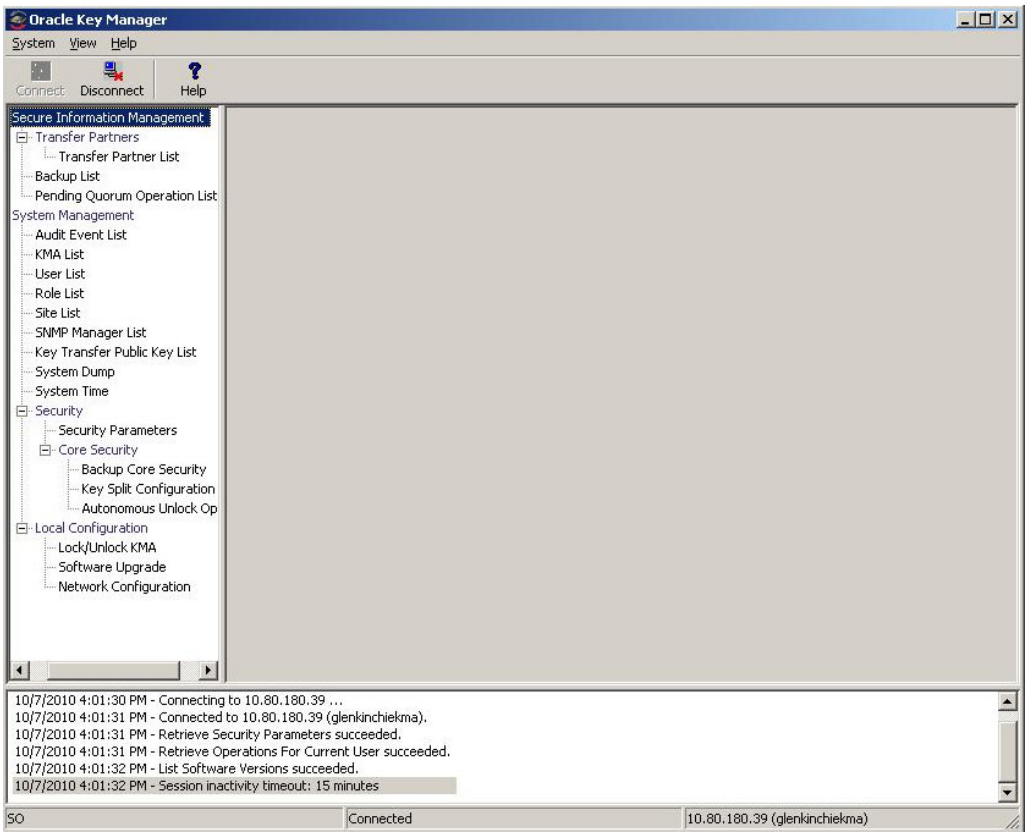
「IP Preference」

必要なインターネットプロトコルバージョンを、「IPv4 only」、「IPv6 only」、または「IPv6 preferred」から選択します。

> **注 ー** クラスタに接続したあとで KMA がそのクラスタに参加した場合、その KMA は「Member KMAs」リストに表示されません。このリストを更新するには、ユーザー名とパスフレーズを入力し、クラスタプロファイルを選択して、「Refresh KMAs」ボタンをクリックします。

重要 ー KMA はユーザー ID とパスフレーズを認証します。返される KMA IP アドレスのリストは、クラスタプロファイルを生成するために使用され、ホスト上に格納されます。次回 KMA に接続するときに、ユーザー名とパスフレーズを入力し、クラスタプロファイルを選択して、KMA を選択できます。

6. 接続が成功した場合は、OKM Manager GUI のステータスバーにユーザー名と別名、KMA の接続ステータス (「**Connected**」)、KMA の IP アドレスが表示されます。



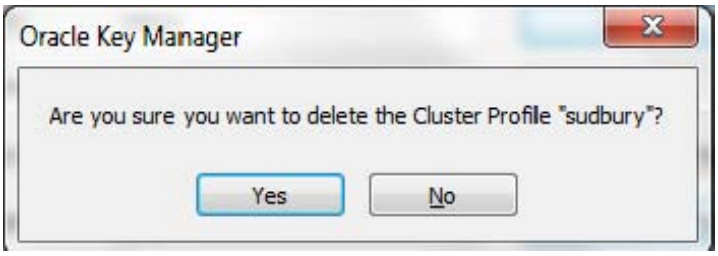
7. これで、OKM Manager を使用してさまざまな操作を実行できるようになりました。さまざまなユーザーの役割が実行できる操作については、第 5 章から第 9 章を参照してください。

注 ー KMA 管理操作のツリー区画に表示されるタスクは、役割の割り当てによって異なります。

クラスタプロファイルの削除

クラスタプロファイルを削除するには、次の手順を実行します。

1. 「Connect to Cluster」ダイアログボックスから、「Cluster Name」フィールドの横にある下矢印ボタンをクリックし、削除するクラスタプロファイルを強調表示して、「Delete Cluster Profile」ボタンをクリックします。「Delete Cluster Profile」ダイアログボックスが表示され、選択したクラスタプロファイルの削除の確認が求められます。



2. 「**Yes**」ボタンをクリックして、プロファイルを削除します。クラスタプロファイルが削除され、「Connect to Cluster」ダイアログボックスに戻ります。

KMA からの切断

KMA から切断するには、次の手順を実行します。

1. 「System」メニューから「**Disconnect**」を選択するか、またはツールバーの 

をクリックします。KMA と OKM クラスタからただちに切り離されます。セッション監査ログ区画に、KMA から切断した日時が表示されます。

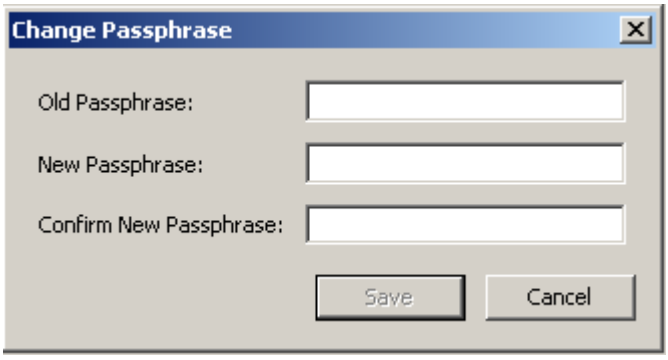
パスフレーズの変更

注 ー このメニューオプションは、プロファイルを使用して KMA に接続されている場合にのみ有効になります。

この機能を使用すると、ユーザーは自分のパスフレーズを変更できます。この機能によって、ユーザーの現在の証明書が無効になることはありません。

接続されているユーザーのパスフレーズを変更するには、次の手順を実行します。

1. 「System」メニューから「**Change passphrase...**」を選択します。「Change passphrase」ダイアログボックスが表示されます。



2. 次のパラメータを入力し、「OK」ボタンをクリックします。

Old Passphrase

ユーザーの現在のパスフレーズを入力します。

New Passphrase

ユーザーの新しいパスフレーズを入力します。

Confirm New Passphrase

同じパスフレーズを再入力します。

3. セッション監査ログ区画に、ユーザーのパスフレーズを変更した日時を示すメッセージが表示されます。

証明書の保存

この機能を使用すると、OKM コマンド行ユーティリティーで使用できる証明書をエクスポートできます (386 ページの「OKM コマンド行ユーティリティー」を参照)。

ルート CA 証明書は PEM 形式で保存された公開証明書であり、PEM ファイルとしてコマンド行インタフェース (CLI) 操作に使用できます。

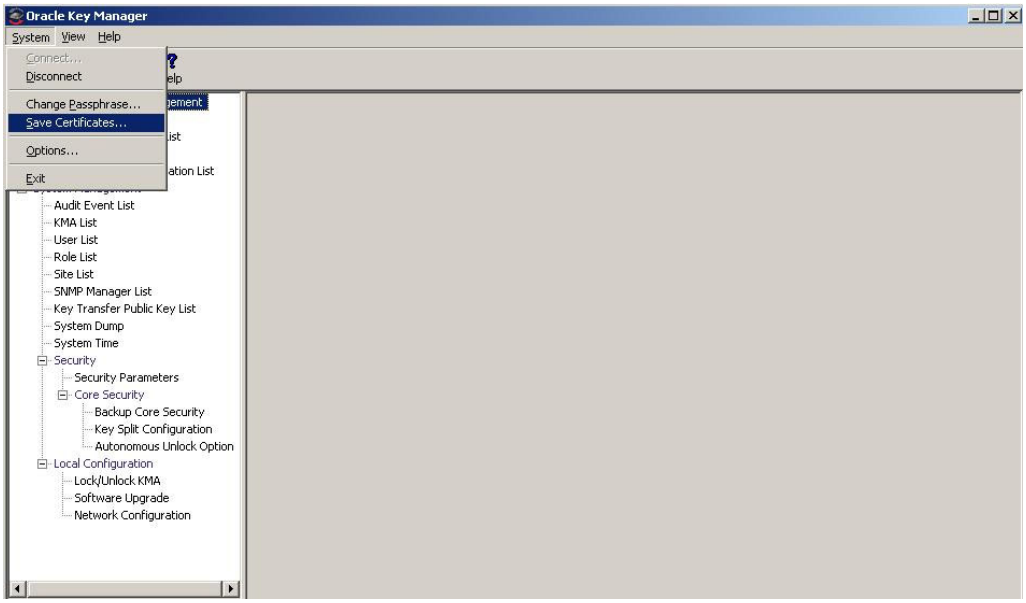
クライアント証明書は、PEM 形式または PKCS12 形式のどちらかで保存できます。PEM 形式には、証明書と暗号化されていない非公開鍵が含まれています。この形式で保存されたクライアント証明書は、PEM ファイルとして CLI 操作に使用できます。

PKCS12 形式は暗号化されています。この形式で保存されたクライアント証明書は、CLI 操作に使用される前に PEM 形式に変換する必要があります (111 ページの「PKCS12 形式から PEM 形式への変換」を参照)。クライアント証明書を PKCS12 形式で保存するには、暗号化に使用するパスワードが必要です。このパスワードには、少なくとも 8 文字が含まれている必要があります。

> **注 ー** これらの証明書ファイルは、ほかのユーザーからのアクセスを制限するのに十分なアクセス権を使用して、安全な場所に格納するようにしてください。**クライアント証明書を PKCS12 形式で保存する場合は、パスワードを保持する必要があります。**

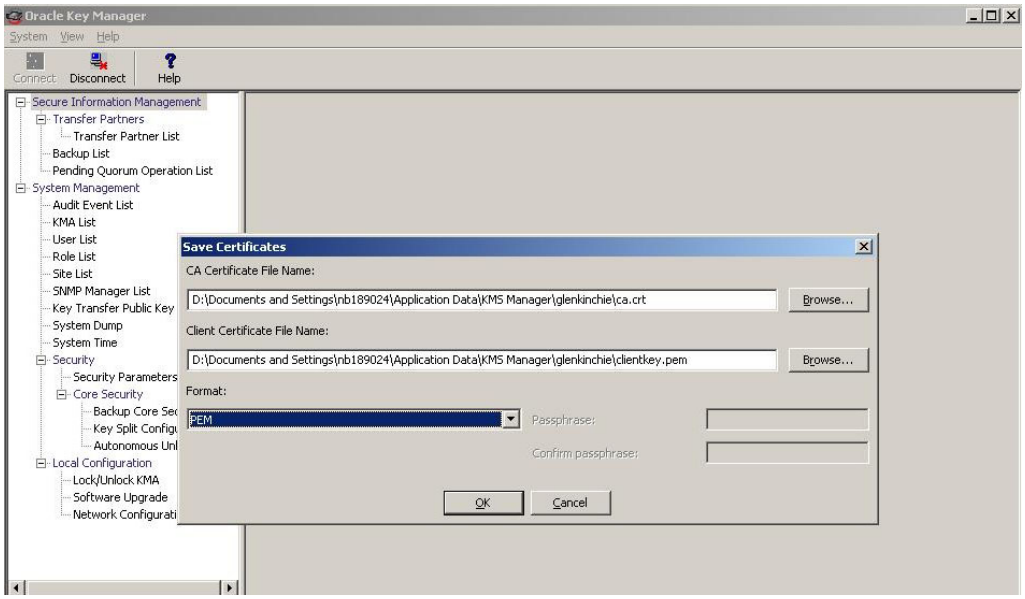
証明書を保存するには、次の手順を実行します。

1. 「System」メニューから「**Save Certificates**」を選択します。



> **注 ー** 「Save Certificates」メニューオプションは、ユーザーが KMA に接続されている場合にのみ有効になります。

「Save Certificates」ダイアログが表示され、ルート CA 証明書とクライアント証明書の自動的に生成されたファイル名が示されます。



これらのファイル名を直接編集するか、または「Browse」をクリックして別の宛先パスを選択したり、ファイル名を編集したりすることができます。

2. 「Format」フィールドで、クライアント証明書がエクスポートされるときの形式を選択します。
3. PKCS12 形式を選択した場合は、「Passphrase」フィールドにパスフレーズを入力し、「Confirm Passphrase」フィールドにこのパスフレーズを再入力します。
4. 「OK」をクリックして、これらの証明書をエクスポートします。これらの証明書がエクスポートされると、これらのファイルの場所を示すメッセージが表示されます。
5. このダイアログを閉じて前の画面に戻るには、「Cancel」をクリックします。

PKCS12 形式から PEM 形式への変換

クライアント証明書を PKCS12 形式で保存した場合は、OKM コマンド行ユーティリティーで使用する前に、その証明書を PEM 形式に変換する必要があります。証明書を変換するには、openssl ユーティリティーを使用します。

openssl ユーティリティーは、OKM Manager GUI と OKM コマンド行ユーティリティーがインストールされたディレクトリの下の OpenSSL ディレクトリにあります。

その構文は次のとおりです。

```
openssl pkcs12 -in PKCS12file -out PEMfile -nodes \
-passin mypassword
```

例:

```
openssl pkcs12 -in KeyTransferOperator.p12 -out
KeyTransferOperator.pem -nodes -passin pass:1234Five
```

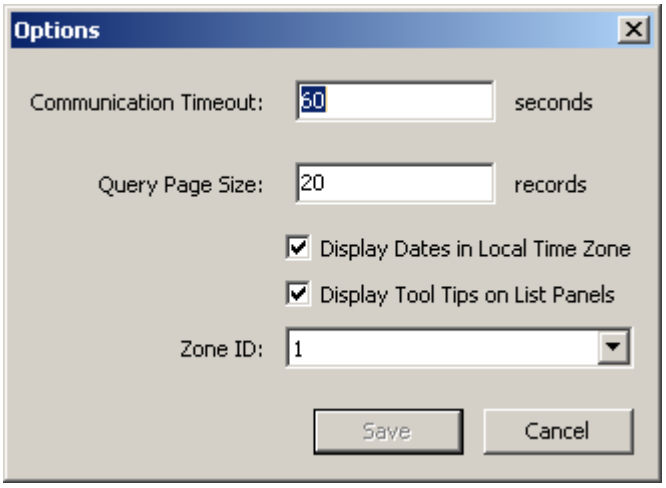
-nodes 引数は、非公開鍵のエクスポートに必要です。非公開鍵はパスワードで保護されていないため、このファイルは適切に管理するようにしてください。

構成設定値の指定

構成設定値を指定するには、次の手順を実行します。

1. 「System」メニューから「**Options...**」を選択します。「Options」ダイアログボックスが表示され、現在の構成設定値が示されます。

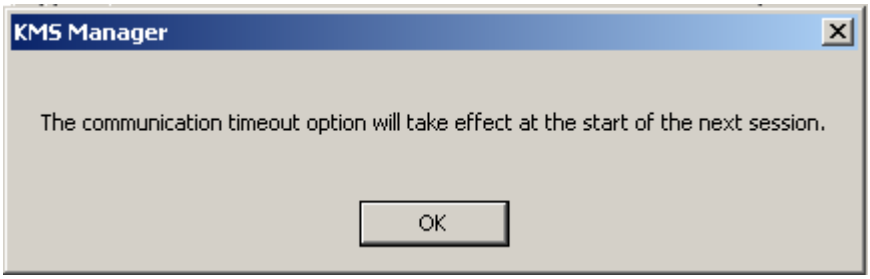
   注 ー 選択されたオプションは、ほかのプラットフォームのために Windows レジストリまたは「`~/.KMS Manager`」(~ はユーザーのホームディレクトリ) に格納されます。これらの値の Windows レジストリキーは、「`My Computer\HKEY_CURRENT_USER\Software\Sun Microsystems\KMS Manager`」です。



2. 必要に応じて次のパラメータを変更し、「**Save**」ボタンをクリックします。

Communication Timeout

接続されている KMA との通信のタイムアウト期間 (秒単位) を入力します。KMA がこのタイムアウト値以内に応答しない場合は、OKM Manager によって通信が切断されます。最小値は 1、最大値は 60 です。デフォルトは 15 分です。



Query Page Size

画面、ダイアログ、または項目リストを表示するダイアログのタブに表示される、項目の最大数を入力します。ページングを使用すると、項目数がこの制限よりも多いリストを表示できます。最小値は 1、最大値は 1000 です。デフォルトは 20 分です。

Display Dates in Local Time Zone

このチェックボックスは、すべての日付と時刻を UTC ではなく、ローカルマシンの (つまり、OKM Manager が実行されている) タイムゾーンで表示する場合に選択します。デフォルトでは選択されています。次の確認メッセージが表示されます。

「Display Tool Tips on List Panels」

このチェックボックスは、カーソルを項目の上に置いたときにツールチップが表示されるようにする場合に選択します。これはデフォルトです。

「Zone ID」

KMA が IPv6 アドレスを持つように構成されており、IPv6 リンクローカルアドレス (つまり、「fe80」で始まる IPv6 アドレス) を使用してそれらの KMA のいずれかに接続する場合は、そのリンクローカルアドレスに接続するときに使用するゾーン ID を選択します。

詳細については、114 ページの「ゾーン ID を含む IPv6 アドレス」を参照してください。

ゾーン ID を含む IPv6 アドレス

Windows システムユーザーの場合は、OKM Manager GUI や、バックアップおよび OKM コマンド行ユーティリティー (385 ページの「コマンド行ユーティリティー」を参照) を使用してリンクローカル IPv6 アドレスを入力できます。ただし、最初にある程度の初期設定を実行する必要があります。

> **注 ー** リンクローカルアドレス (つまり、「fe80」で始まる IPv6 アドレス) を指定する場合は常に、ゾーン ID を入力する必要があります。ゾーン ID は、IPv6 アドレスの最後にパーセント記号 (%) に続けてその ID を追加することによって指定できます。

1. コマンドプロンプトウィンドウを表示し、Windows システム上でどのゾーン ID が使用可能かを確認します。

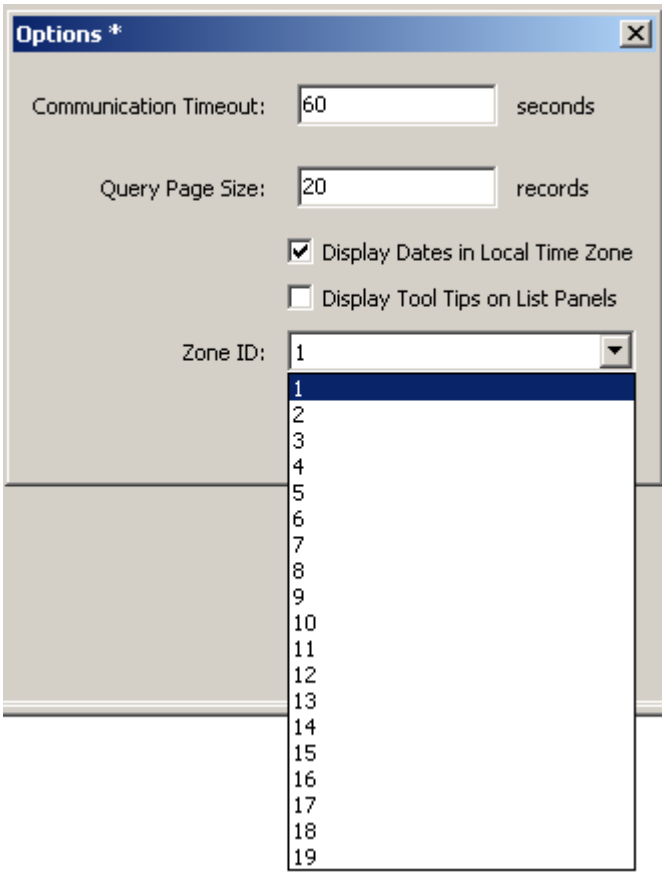
```
netsh interface ipv6 show interface
```

   ゾーン ID は、このコマンドの出力にある「Idx」列に表示されます。「Connected」の状態を示すエントリを探します。

2. ping コマンドを使用して、これらのゾーン ID のいずれかを使用したネットワーク接続を確認します。次に例を示します。

```
ping fe80::216:36ff:fed5:fba2%4
```

3. OKM Manager GUI で「Connect」ダイアログを表示する前に、「Options」ダイアログを表示し、適切なゾーン ID を選択します。



4. 「**Save**」ボタンをクリックします。

OKM Manager の終了

OKM Manager を終了するには、次の手順を実行します。

1. 「System」メニューから「**Exit**」を選択するか、またはタイトルバーの  をクリックします。OKM Manager が終了し、Windows のデスクトップに戻ります。
2. OKM Manager が接続されている場合は、ただちに切り離されて終了します。

5

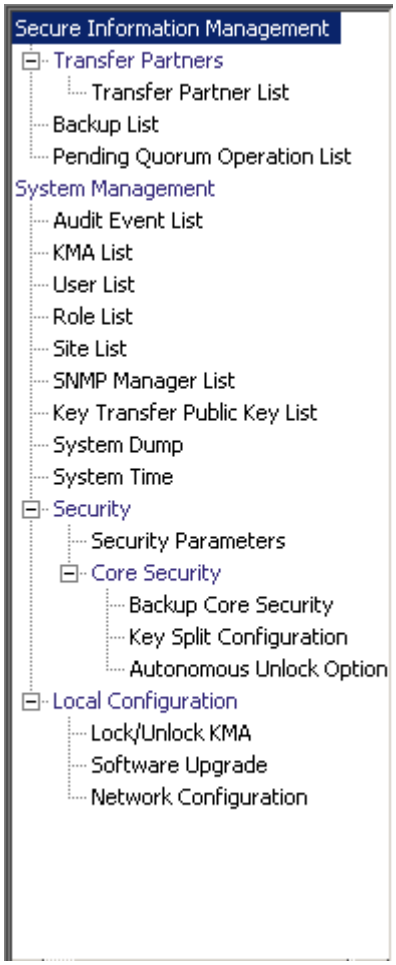
セキュリティー責任者の操作

セキュリティー責任者は、セキュリティー設定、ユーザー、サイト、および転送パートナーを管理します。この章では、次の項目について説明します。

- セキュリティー責任者の役割が付与されたユーザーが実行できる操作。複数の役割が割り当てられている場合は、その役割を実行する手順について、該当する章を参照してください。
- 技術サポートアカウントを有効および無効にする手順。

セキュリティー責任者の役割

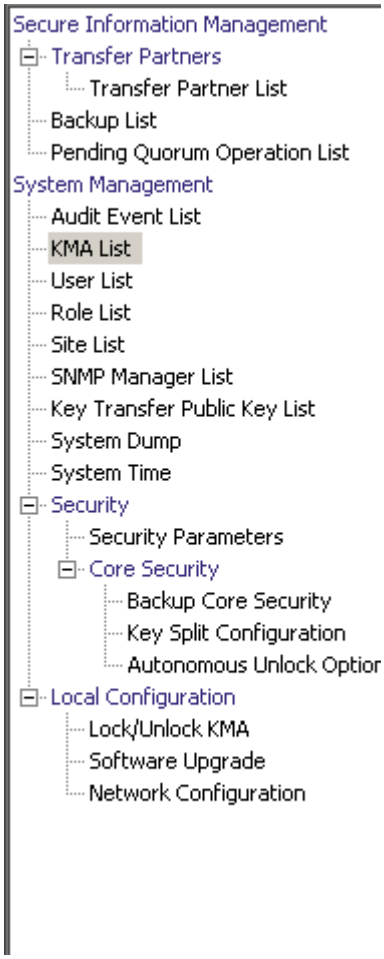
セキュリティー責任者は、実体 (KMA、ユーザー、サイト、転送パートナー) およびシステムのさまざまなセキュリティーの側面を管理できます。



「KMA List」メニュー

「KMA List」メニューオプションを使用すると、次の操作を行うことができます。

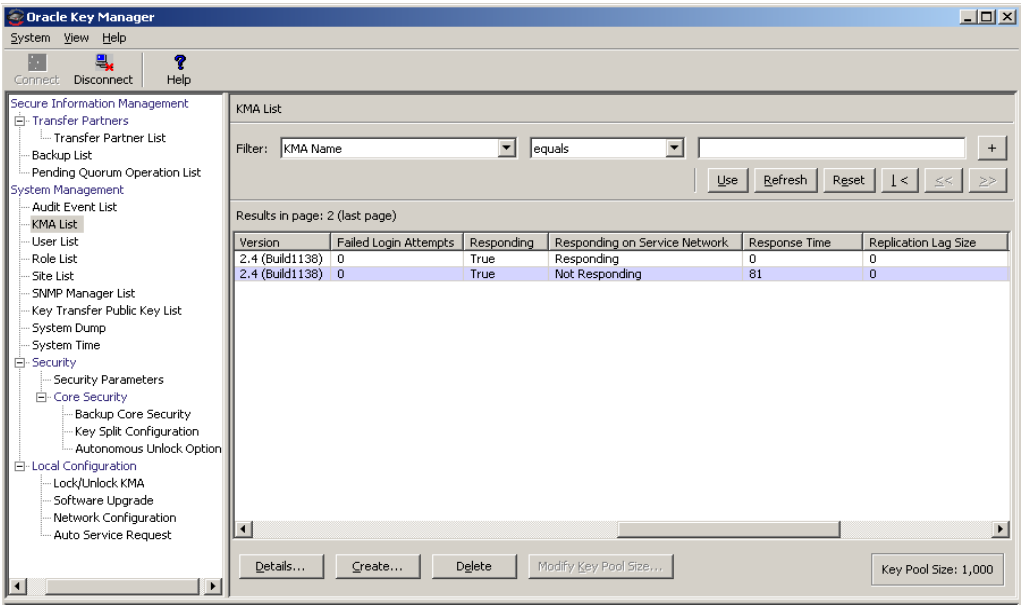
- KMA の表示
- KMA の作成
- KMA の情報の変更
- KMA の削除
- 鍵プールのサイズ変更 (331 ページの「鍵プールサイズの変更」を参照) これはバックアップオペレータの機能です。



KMA の表示

KMA を表示するには、次の手順を実行します。

「System Management」メニューから、「**KMA List**」を選択します。「KMA List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで KMA リストにフィルタを適用することもできます。

- KMA 名
- 説明
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- バージョン
- Failed Login Attempts
- Enrolled

表示されている KMA リストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ：

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- KMA 名
- 説明
- Site ID
- Management Network Address
- Service Network Address
- Management Network Address (IPv6)
- Service Network Address (IPv6)
- バージョン
- Failed Login Attempts
- Enrolled

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス :

このフィールドに値を入力します。

使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

KMA 名

クラスタ内の各 KMA を識別するユーザー指定の識別子が表示されます。

KMA ID

KMA を識別する一意のシステム生成識別子が表示されます。

説明

KMA の説明が示されます。

Site ID

KMA が属するサイトが示されます。

Management Network Address

管理ネットワークでの KMA の IP アドレスが表示されます。

Service Network Address

サービスネットワークでの KMA の IP アドレスが表示されます。

Management Network Address (IPv6)

管理ネットワークでの KMA の IPv6 アドレス (ある場合) が表示されます。

Service Network Address (IPv6)

サービスネットワークでの KMA の IPv6 アドレス (ある場合) が表示されます。

バージョン

KMA ソフトウェアのバージョン番号が表示されます。

Failed Login Attempts

ログオンに失敗した回数が表示されます。

Responding

KMA が動作中かどうかが示されます。True または False の値を取ります。

Responding on Service Network

サービスネットワークで KMA が応答しているかどうかを示します。取り得る値は「Responding」、「Not Responding」、または「Not Accessible」です。

- **Responding** は、この OKM が接続している KMA (ローカル KMA) からの要求に KMA が応答していることを示します。この状態はクラスタ内の KMA のすべてのペア間に該当しますが、表示される値は、リスト内の個々の KMA (リモート KMA) がローカル KMA からの要求に応答しているかどうかを示します。
- **Not Responding** は、リモート KMA、またはリモート KMA への通信リンクがダウンしているなどの原因で、リモート KMA が要求に応答していないことを示します。
- **Not Accessible** は、サービスネットワーク構成でリモート KMA へのデフォルト経路または静的経路が指定されていないなどの原因で、リモート KMA がローカル KMA にアクセスできないことを示します。

  注 ー ローカル KMA でデフォルト経路が構成されている場合、その KMA はリモート KMA への経路を備えているものとみなされます。サービスネットワークでほかの KMA が応答していない場合、それらの KMA は「Not Responding」と表示されます。デフォルト経路または静的経路が定義されていない場合、ほかの KMA が「Not Accessible」と表示されることがあります。

  古い KMA (OKM 2.3.*x* 以前) は「Responding」と表示されます。

Response Time

KMA が要求に応答するまでの時間がミリ秒単位で表示されます。

Replication Lag Size

複製を待機している更新の数が表示されます。

Key Pool Ready

使用可能な未割り当ての鍵のパーセンテージが表示されます。

Key Pool Backed Up

バックアップが完了した鍵プールのパーセンテージが表示されます。

Locked

KMA がロックされているかどうかを示します。

注 ー KMA がこれらの機能をサポートしない場合、「**Key Pool Backed Up**」および「**Locked**」フィールドには値「N/A」が表示されます。

Enrolled

KMA が追加されているかどうか、または KMA がクラスタに正常にログインしているかどうかが示されます。True または False の値を取ります。

HSM Status

ハードウェアセキュリティーモジュール (HSM) の状態を示します。取り得る値は Unknown、Inactive、Software、Hardware、SW Error、または HW Error です。

不明

KMA は OKM 2.3 よりも古いソフトウェアリリースを実行しています。

無効

KMA では現在、HSM を使用する必要がありません。これは通常、KMA がロックされていることが原因です。

ソフトウェア

HSM は正常に動作しておらず、KMA はソフトウェアプロバイダを使用して鍵を生成しています。

ハードウェア

HSM は正常に動作しており、KMA は HSM を使用して鍵を生成しています。

SW Error/HW Error

KMA でソフトウェアプロバイダ (SW Error) または HSM (HW Error) の状態を確認しようとしたときにエラーが発生しました。

注 ー

通常は、HSM は正常に動作しています (Hardware)。ただし、HSM が正常に動作しなくなり (Software)、「FIPS Mode Only」セキュリティーパラメータが Off に設定 (207 ページの「セキュリティーパラメータの取り出し」を参照) されている場合、KMA はソフトウェアプロバイダを使用して鍵を生成する動作に切り替わります。

HSM が正常に動作しなくなり、「FIPS Mode Only」セキュリティーパラメータが On に設定されている場合、KMA は鍵を生成できないか、または AES でラップされた鍵データをエージェントに返すことができません。

値が Software、SW Error、または HW Error の場合は、この KMA 上の Sun Crypto Accelerator (SCA) 6000 カードを確認してください (「SCA 6000 カードの確認」を参照)。

SCA 6000 カードの確認

クラスタ内の既存の KMA に装着された SCA 6000 カードが故障している可能性があります。故障したカードを特定するには、KMA サーバーの背面を調べて、カードの LED を確認します。

QuickStart プログラムによって初期化され、KMS 2.1、2.2、または OKM 2.3 以降の KMA で正常に動作している SCA 6000 カードは、(S と表記された) 状態表示 LED が緑色に点滅し、FIPS (F) および初期化 (I) LED が緑色に点灯しています。

状態表示 LED が緑色の点滅でなく、FIPS および初期化 LED が緑色の点灯でない場合、KMA の SCA 6000 カードは故障しており、FIPS モードが必要な場合は KMA を交換する必要があります。

SCA 6000 カードの LED については、『SCA 6000 User Guide』を参照してください。

KMA を作成する場合は、「Create」ボタンをクリックします。詳細は、126 ページの「KMA の作成」を参照してください。

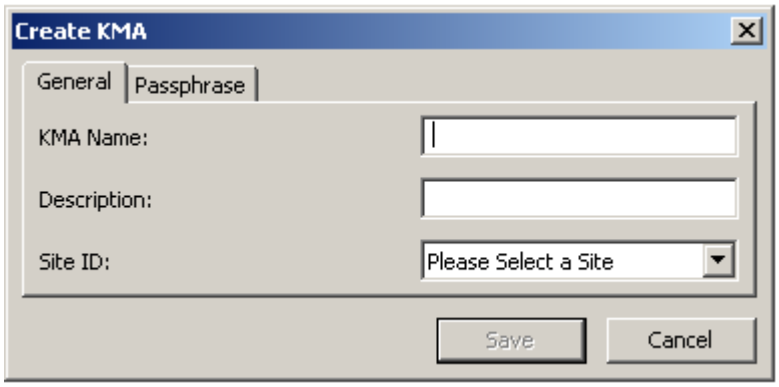
KMA の詳細を表示または変更する場合は、その KMA を強調表示して「Details」ボタンをクリックします。詳細については、129 ページの「KMA の詳細の表示および変更」を参照してください。

KMA を削除する場合は、「Delete」ボタンをクリックします。詳細については、135 ページの「KMA の削除」を参照してください。

KMA の作成

KMA を作成するには、次の手順を実行します。

1. 「KMA List」画面で、「**Create**」ボタンをクリックします。「Create KMA」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブで、必要に応じて次の情報を指定します。

KMA 名

クラスタ内の KMA を一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

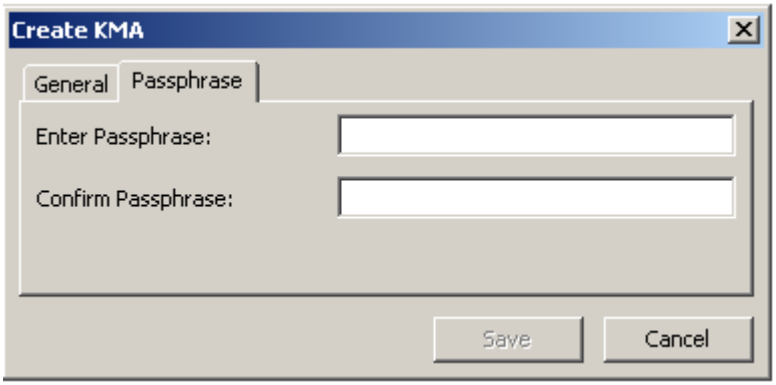
説明

KMA を一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Site ID

下矢印ボタンをクリックし、KMA が属するサイトを選択します。このフィールドは省略可能です。

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定し、「**Save**」ボタンをクリックします。

Enter Passphrase

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーの KMA 名を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

  使用可能な特殊文字は、次のとおりです。

  ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?

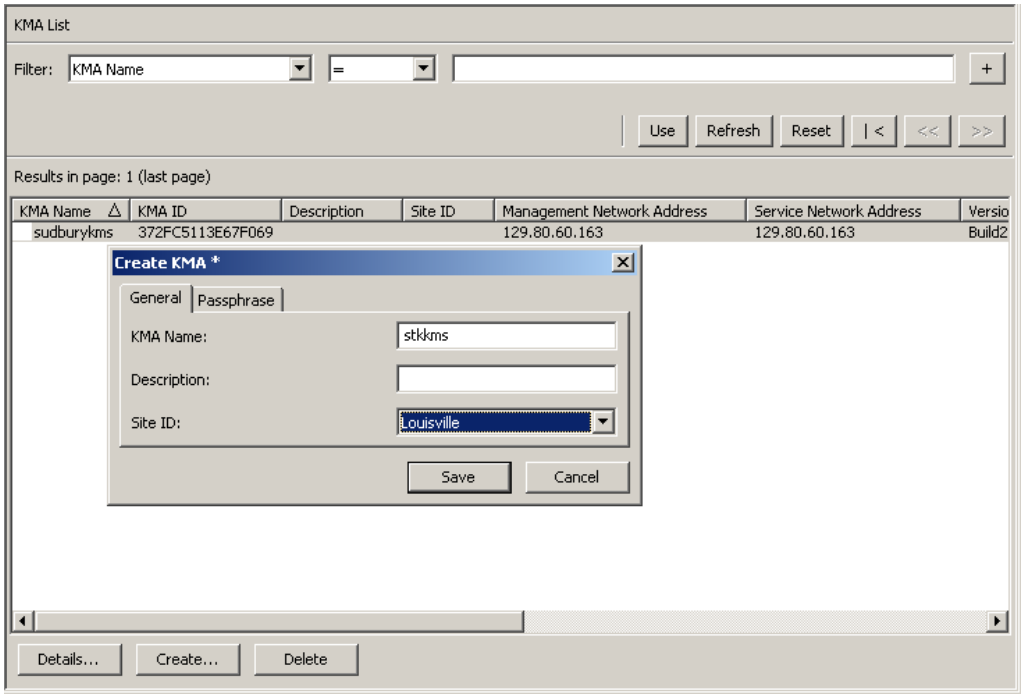
- タブ、改行などの制御文字は使用できません。

  注 – パスフレーズの最小文字数の要件を変更する方法については、211 ページの「セキュリティーパラメータの変更」を参照してください。

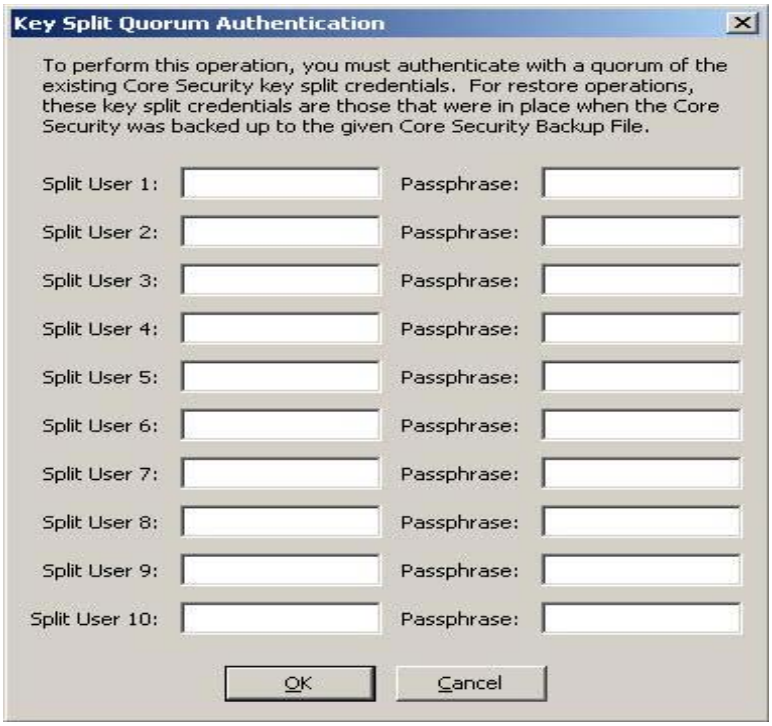
Confirm Passphrase

「**Enter Passphrase**」フィールドに入力した値と同じ値を入力します。

5. KMA レコードがデータベースに追加され、そのエントリが「KMA List」画面に表示されます。



6. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「Save」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

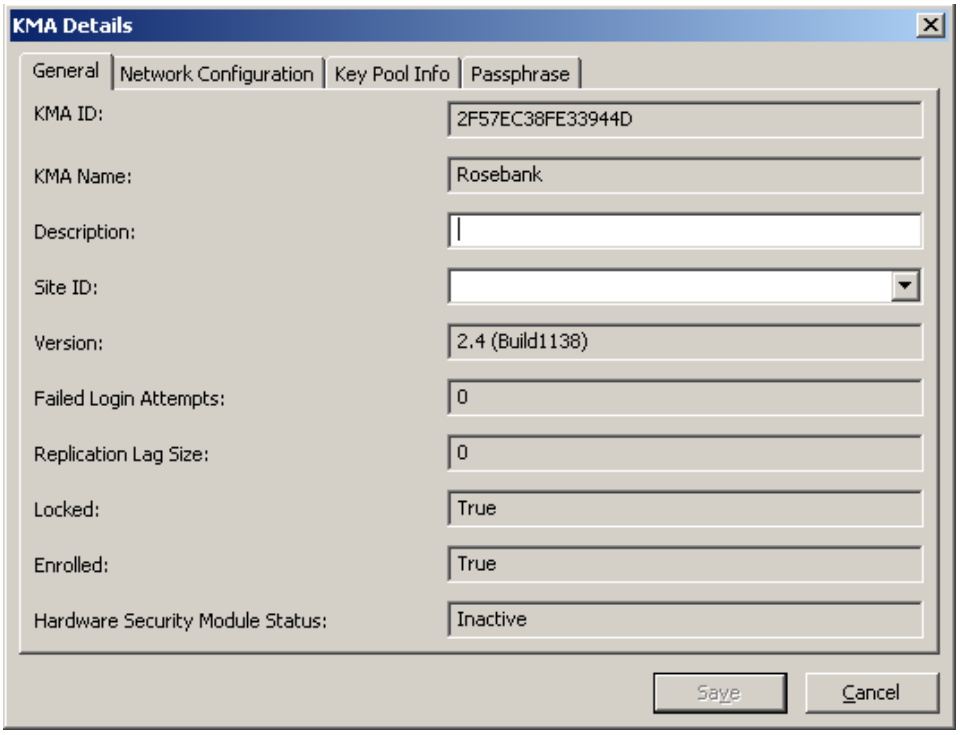
7. 作成した KMA で QuickStart プログラムを実行し、KMA がクラスタに参加できるようにします。クラスタへの参加の手順については、65 ページの「既存のクラスタへの参加」を参照してください。

KMA の詳細の表示および変更

注 ー セキュリティー責任者以外のユーザーが KMA の詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

KMA の詳細を変更するには、次の手順を実行します。

1. 「KMAs List」画面で、詳細情報を表示する KMA 項目をダブルクリックするか、または KMA エントリを強調表示して「**Details**」ボタンをクリックします。「KMA Details」ダイアログボックスが表示されます。

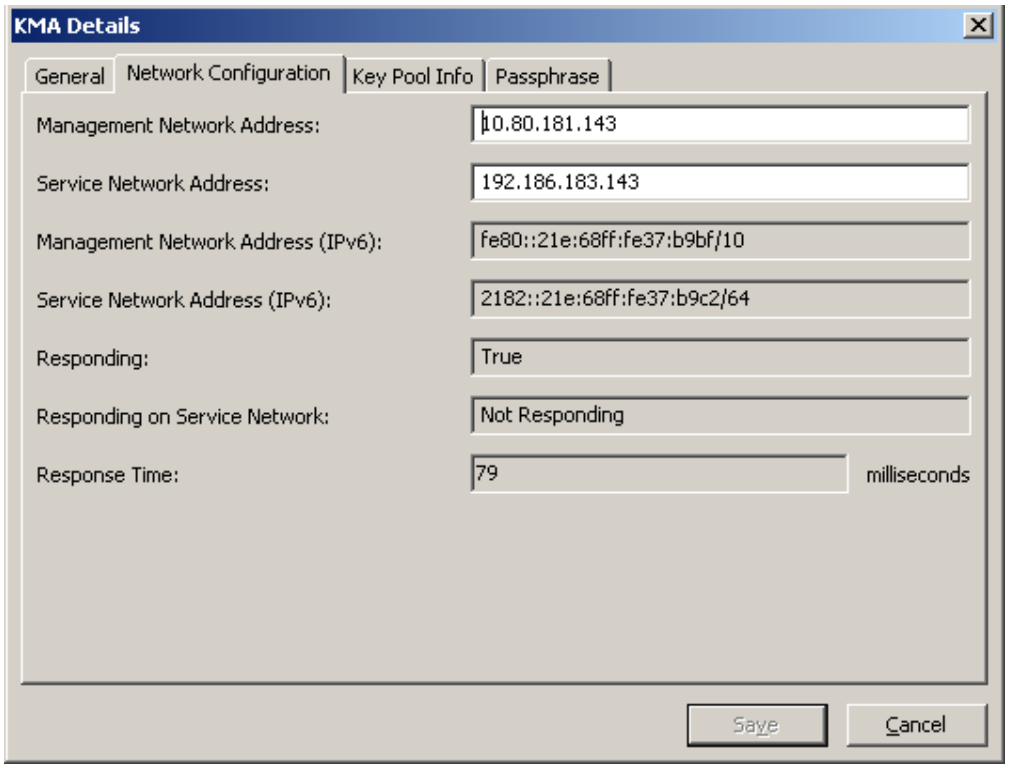


2. 「General」タブで、次のフィールドを変更します。

- 説明
- Site ID

3. 「Network Configuration」タブで、次のフィールドを変更します。

- Management Network Address
- Service Network Address.



4. 「Key Pool Info」タブには、次の表示専用フィールドがあります。

Ready Keys

この KMA で生成され、バックアップ (単一ノードクラスタの場合) またはほかの KMA に複製 (複数ノードクラスタの場合) されたが、まだ暗号化のためにエージェントに渡されていない鍵の数が表示されます。

Backup-Up Ready Keys

鍵プール内の使用可能な鍵のうち、バックアップが完了したものの数が表示されます。N/A は、ダウンレベルのソフトウェアを KMA で実行しているか、または KMA で現在使用している複製バージョンのほうが低いことが原因で、KMA がこの値を特定できないことを意味します。

Generated Keys

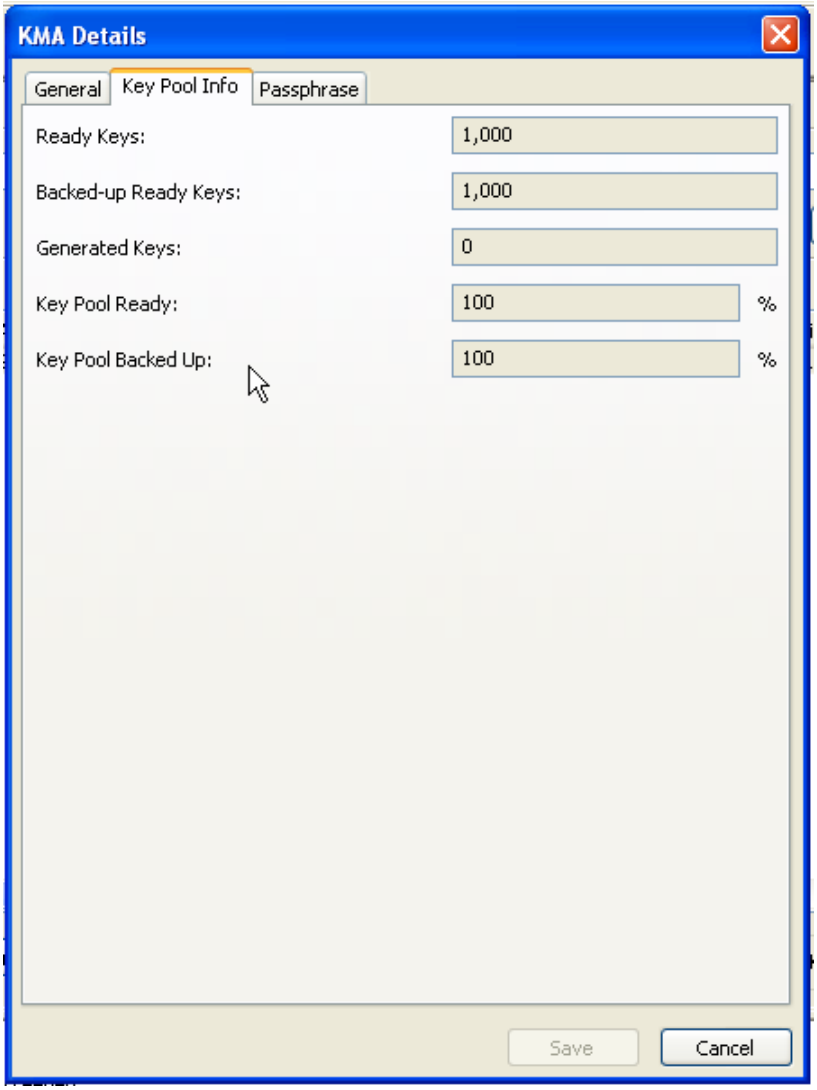
この KMA で生成されたが、まだバックアップ (単一ノードクラスタの場合) またはほかの KMA に複製 (複数ノードクラスタの場合) されていない鍵の数が表示されます。

Key Pool Ready

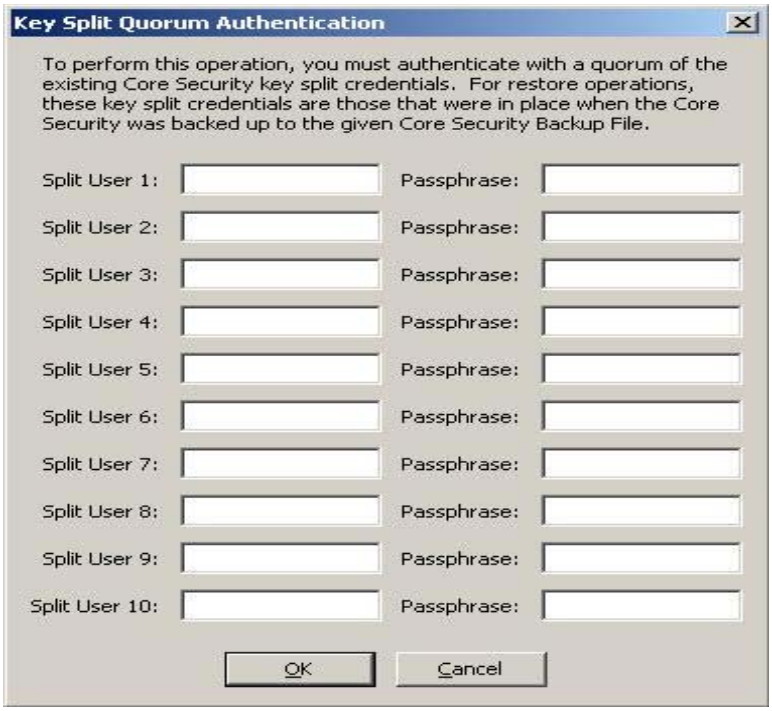
鍵プール内の鍵のうち、使用可能なもののパーセンテージが表示されます。

Key Pool Backed Up

鍵プール内の使用可能な鍵のうち、バックアップが完了したもののパーセンテージが表示されます。N/A は、ダウンレベルのソフトウェアを KMA で実行しているか、または KMA で現在使用している複製バージョンのほうが低いことが原因で、KMA がこの値を特定できないことを意味します。



5. 「Passphrase」タブを開き、次のパラメータを変更します。
   - パスフレーズ
   - Confirm Passphrase (同じパスフレーズを再入力)
6. 終了したら、「**Save**」ボタンをクリックします。データベース内の KMA レコードが変更されます。
7. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

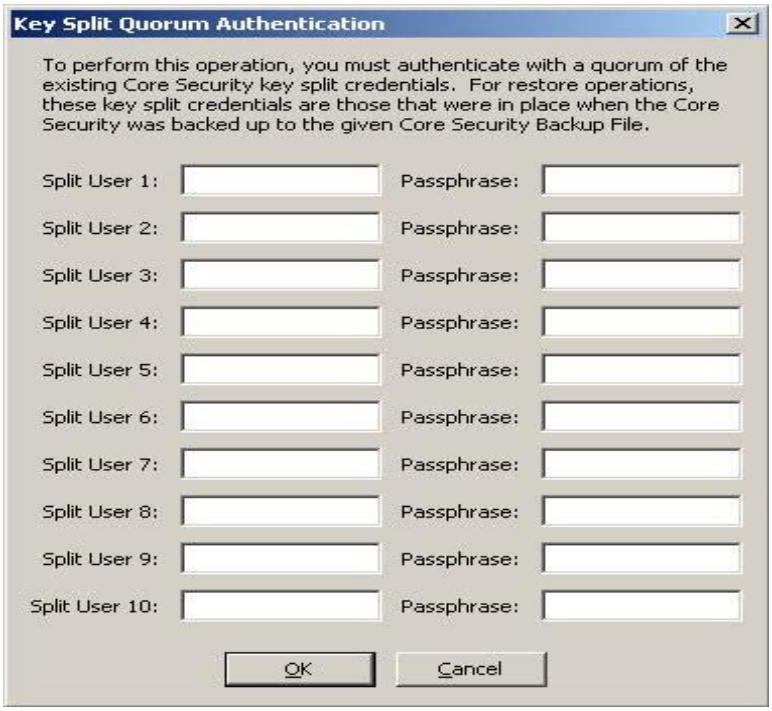
KMA のパスフレーズの設定

注 ー KMA に接続されていない場合に、KMA のパスフレーズを変更できます。

新しいクラスタを作成する場合、新しいクラスタの作成に使用される KMA には、ランダムなパスフレーズが自動的に割り当てられます。証明書の期限切れによって、KMA が実体の証明書をクラスタ内の別の KMA から取得する必要がある場合には、この機能を使用して、パスフレーズを既知の値に設定します。

KMA のパスフレーズを設定するには、次の手順に従います。

1. 「KMAs List」画面で、KMA エントリをダブルクリックするか、または KMA エントリを強調表示して「**Details**」ボタンをクリックします。「KMA Details」ダイアログボックスが表示され、「General」タブがアクティブになっています。
2. 「Passphrase」タブを開き、次のパラメータを変更します。
   - パスフレーズ
   - Confirm Passphrase (同じパスフレーズを再入力)
3. 「**Save**」ボタンをクリックして、変更内容を保存します。KMA のデータベースエントリが変更されます。
4. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「Save」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

5. コンソールを使用して、パスフレーズが変更された KMA で、KMA をクラスタにログインさせる機能を選択します。再度ログインするまで、KMA はクラスタと通信できません。

   注 ー 数時間以上にわたって KMA がクラスタからログアウトしている場合は、KMA を再度クラスタにログインさせる前に KMA をロックしてください。

   「KMA List」パネルで「Replication Lag Size」に示されるように、最近の更新がこの KMA に伝播されてから、KMA をロック解除します。

   詳細は、次の各項目を参照してください。

   - 222 ページの「Lock/Unlock KMA」
   - 119 ページの「「KMA List」メニュー」
   - 360 ページの「KMA のクラスタへの再ログイン」.

KMA の削除

重要 – KMA を削除する前に、コンソールの「Shutdown KMA」機能を使用して、KMA をオフラインにする必要があります。KMA をオフラインにしておかないと、KMA はクラスタ外で機能し続けて、エージェントとユーザーに「古い情報」を送信します。

通常、このコマンドは、クラスタから障害のある KMA を削除する場合にのみ使用されます。ただし、使用しなくなった KMA を削除するために使用されることもあります。しかし、このような場合には、コンソールの「Reset KMA」機能でゼロ化オプションを使用することをお勧めします。この機能は、クラスタから KMA を削除し、使用しなくなった KMA のディスクからすべての情報を完全に消去します。

削除した KMA をクラスタに再度参加させる場合は、KMA を出荷時のデフォルトにリセットし、QuickStart プログラムからオプション 2 を選択する必要があります。

このオプションを使用すると、セキュリティー責任者は、使用していない KMA を削除できます。

KMA を削除するには、次の手順を実行します。

1. 「KMAs List」画面で、削除する KMA を強調表示して「**Delete**」ボタンをクリックします。次のように、選択した KMA の削除を確認するダイアログボックスが表示されます。

2. 「**Yes**」ボタンをクリックして、KMA を削除します。現在選択している KMA が削除され、「KMA List」画面に戻ります。また、この KMA に関連付けられていて、その他の実体では使用されていないエントリもすべて削除されます。

「User List」メニュー

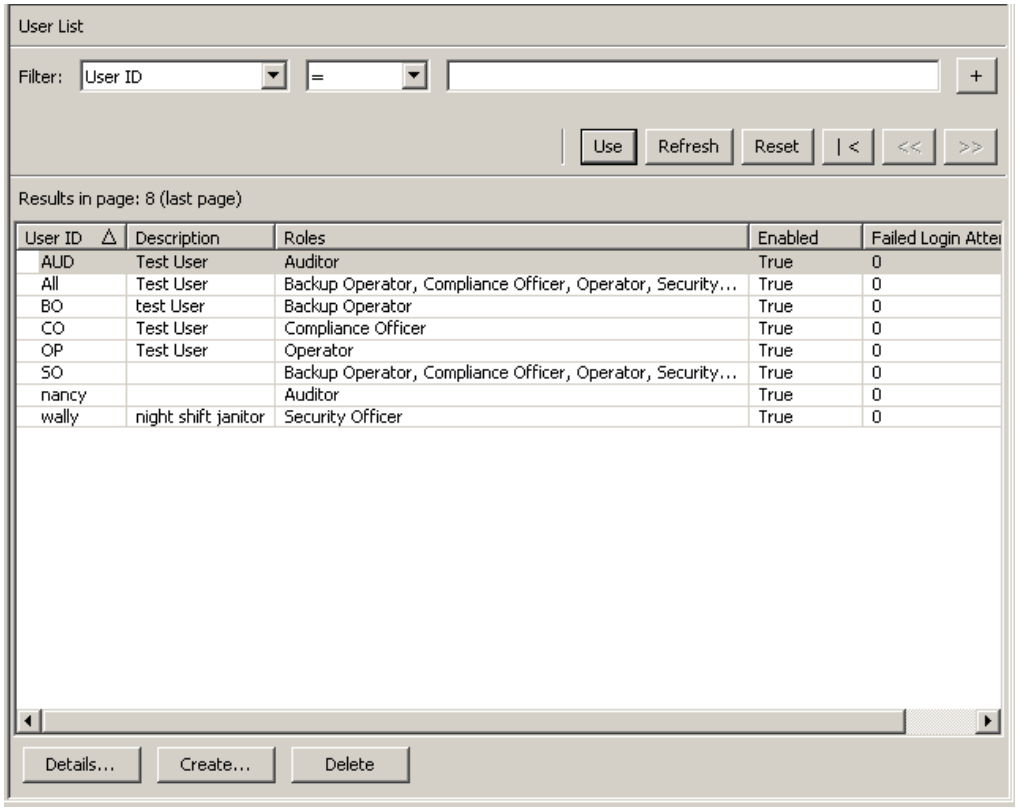
「User List」メニューオプションを使用すると、次の操作を行うことができます。

- ユーザーの表示
- ユーザーの作成
- 既存のユーザー情報の変更
- 既存のユーザーの削除

ユーザーの表示

ユーザーを表示するには、次の手順を実行します。

「System Management」メニューから、「**User List**」を選択します。「User List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでユーザーリストにフィルタを適用することもできます。

- ユーザー ID
- 説明
- 役割
- 有効
- Failed Login Attempts

表示されているユーザーリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- ユーザー ID
- 説明
- 有効
- Failed Login Attempts

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス :

このフィールドに値を入力します。

使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

ユーザー ID

クラスタ内の各ユーザーを識別する一意の識別子が表示されます。これは通常、「ユーザー名」と呼ばれます。

説明

ユーザーの説明が示されます。

役割

ユーザーのセキュリティー役割のリストが表示されます。役割によって、ユーザーはさまざまな操作を実行できます。

有効

ユーザーのステータスが示されます。True または False の値を取ります。

Failed Login Attempts

ログインに失敗した回数が示されます。

ユーザーを作成する場合は、「Create」ボタンをクリックします。詳細については、140 ページの「ユーザーの作成」を参照してください。

ユーザーの詳細を変更する場合は、そのユーザーを強調表示して「Details」ボタンをクリックします。詳細については、143 ページの「ユーザーの詳細の表示および変更」を参照してください。

ユーザーを削除する場合は、「Delete」ボタンをクリックします。詳細については、147 ページの「ユーザーの削除」を参照してください。

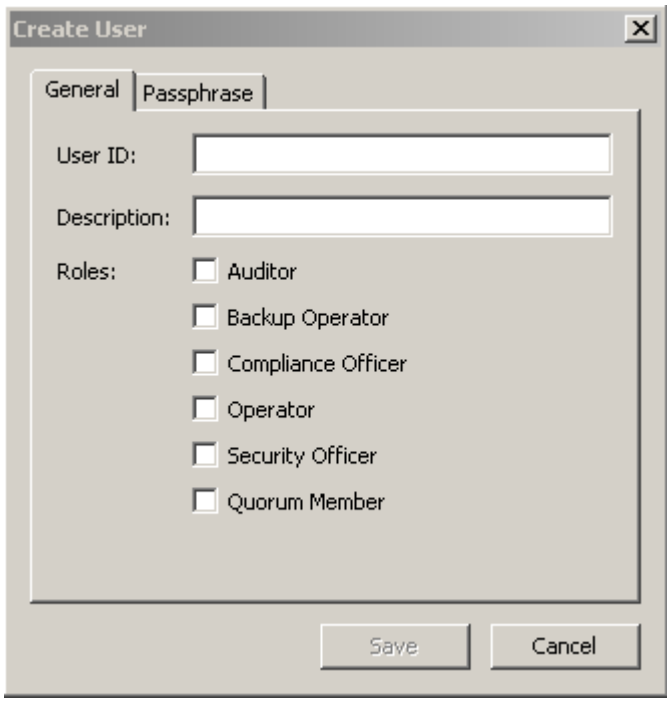
ユーザーのパスフレーズまたは証明書、あるいはその両方が危殆化されている場合、セキュリティー責任者は、ユーザーのパスフレーズを設定できます。ユーザーのパスフレーズを設定する手順については、145 ページの「ユーザーのパスフレーズの設定」を参照してください。

また、ユーザーが自身のパスフレーズを変更することもできます。手順については、108 ページの「パスフレーズの変更」を参照してください。

ユーザーの作成

ユーザーを作成するには、次の手順を実行します。

1. 「User List」画面で、「**Create**」ボタンをクリックします。「Create User」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブ

ユーザー ID

ユーザーを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

説明

ユーザーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

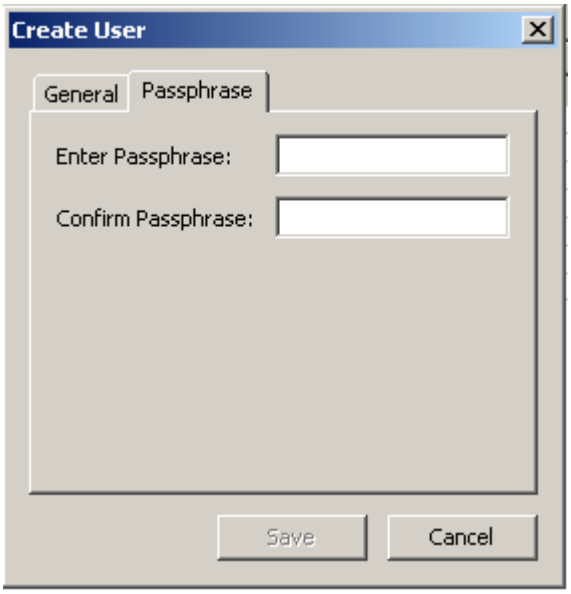
役割

ユーザーに付与する役割の横にあるチェックボックスを選択します。

> **注 ー** バージョン 2.1 以前の KMS ソフトウェアを現在 KMS で実行しているか、または OKM クラスタの複製バージョンが現在 10 またはそれ以下に設定されている場合、「Quorum Member」チェックボックスは使用不可であり、グレー表示されます。

「Passphrase」タブ

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定します。

パスフレーズ

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーのユーザー ID を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

使用可能な特殊文字は、次のとおりです。

‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?

- タブ、改行などの制御文字は使用できません。

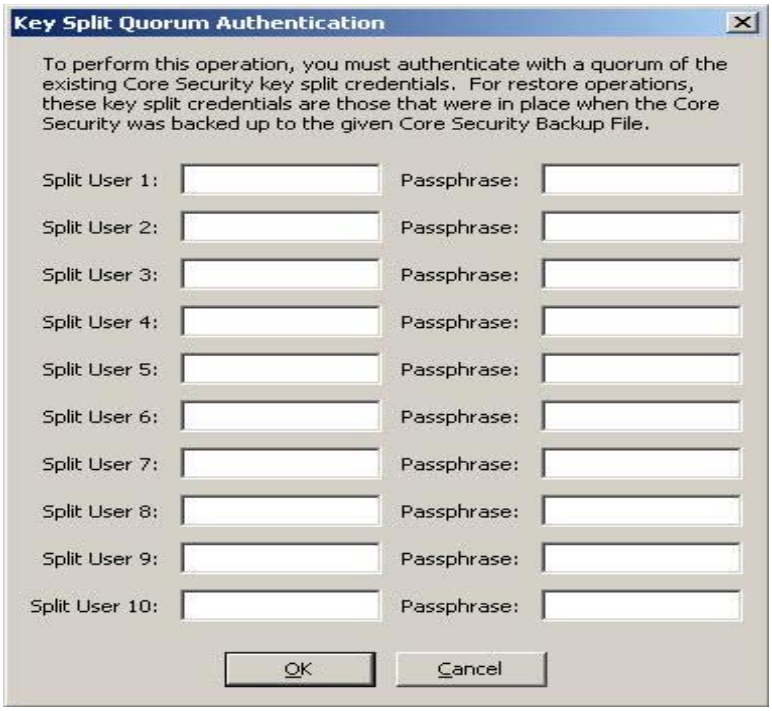
注 ー パスフレーズの最小文字数の要件を変更する方法については、211 ページの「セキュリティーパラメータの変更」を参照してください。

Confirm Passphrase

「Enter Passphrase」フィールドに入力した値と同じ値を入力します。

5. 「**Save**」ボタンをクリックします。ユーザーレコードがデータベースに追加されます。新しいユーザーが「User List」に表示されます。

6. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「Save」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

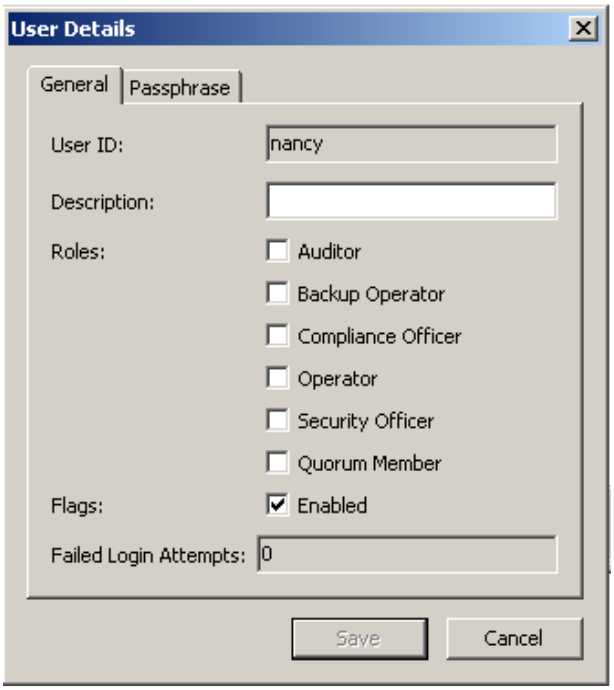
複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

ユーザーの詳細の表示および変更

注 ー 現在ログインしているセキュリティー責任者は、自身のレコードを変更できません。

ユーザー情報を変更するには、次の手順を実行します。

1. 「Users List」画面で、詳細情報を表示するユーザーをダブルクリックするか、またはユーザーレコードを強調表示して「**Details**」ボタンをクリックします。「User Details」ダイアログボックスが表示され、「**Save**」ボタンを含むすべてのフィールドが使用不可になっています。

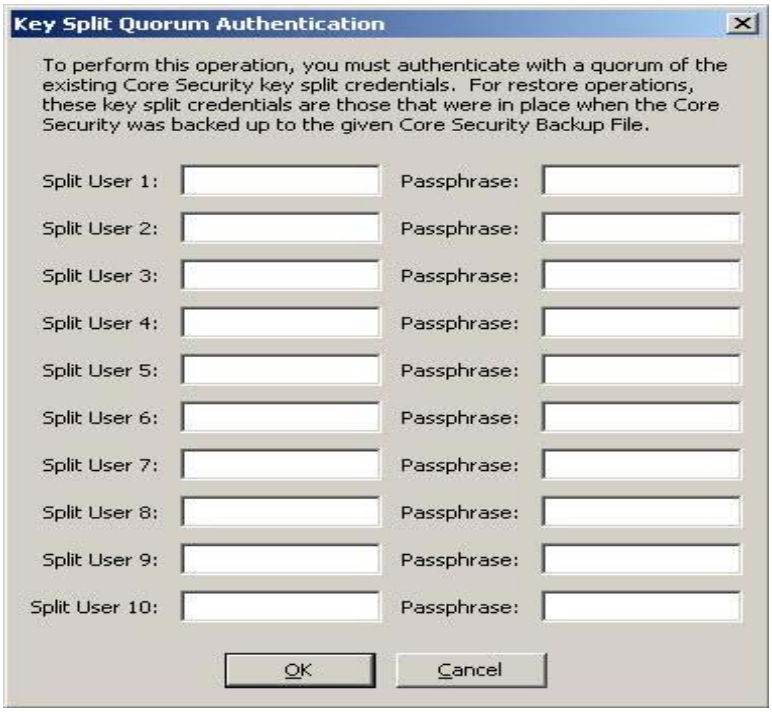


2. 「General」タブで、次のパラメータを変更します。
   - 説明
   - 役割
   - Flags - Enabled

「Failed Login Attempts」フィールドには、ログインに失敗した回数が表示されます。

3. 「Passphrase」タブでユーザーのパスフレーズを変更する場合は、145 ページの「ユーザーのパスフレーズの設定」を参照してください。
4. 終了したら、「**Save**」ボタンをクリックします。
5. ユーザーの役割を追加した場合、「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。

注 ー ユーザーの役割を追加しなかった場合、「**Save**」ボタンをクリックしたあとに OKM クラスタでユーザー情報が更新され、「Key Split Quorum Authentication」ダイアログボックスは表示されません。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「Save」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

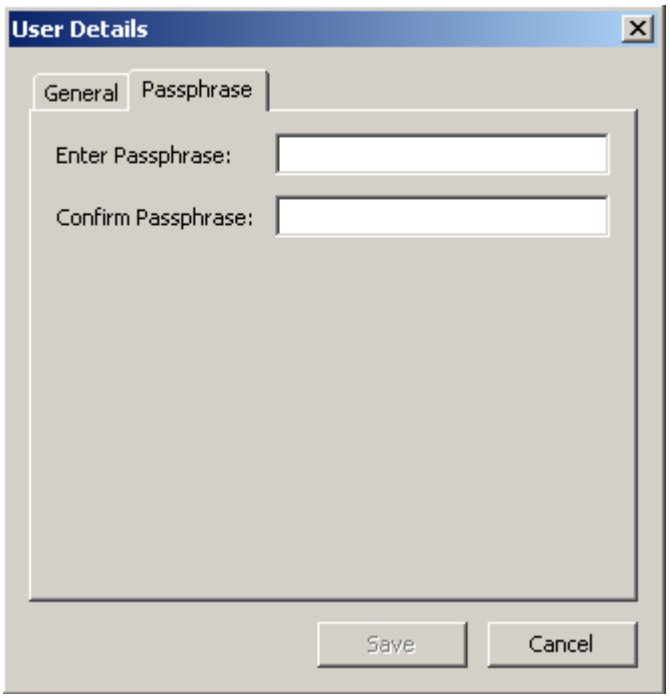
複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

ユーザーのパスフレーズの設定

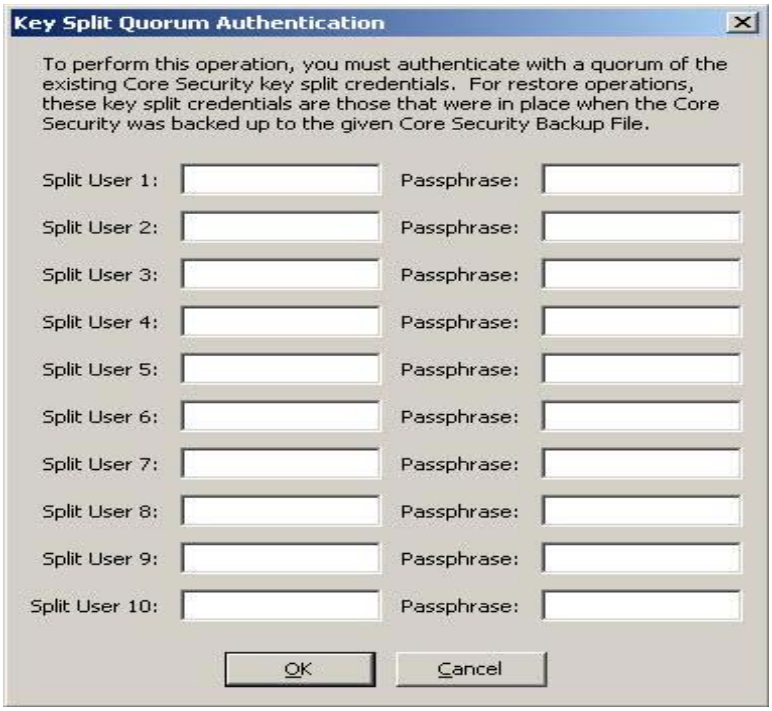
ユーザーのパスフレーズまたは証明書、あるいはその両方が危殆化されていると思われる場合、セキュリティー責任者は、ユーザーのパスフレーズを設定できます。ユーザーが新しいパスフレーズを使用して KMA にログオンすると、新しい証明書が生成されます。

ユーザーのパスフレーズを設定するには、次の手順を実行します。

1. 「Users List」画面で、パスフレーズを選択するユーザーをダブルクリックするか、またはユーザーを強調表示して「**Details**」ボタンをクリックします。
2. 「User Details」ダイアログボックスが表示されます。「Passphrase」タブを開きます。



3. 「**Enter Passphrase**」フィールドで、ユーザーアカウントの作成時にセキュリティー責任者によって割り当てられたパスフレーズを入力します。
4. 「**Confirm Passphrase**」フィールドに、手順 3 で入力した値と同じ値を入力します。ユーザーレコードの新しいパスフレーズが保存されます。
5. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

ユーザーの削除

ユーザーは、ユーザー自身を削除できません。

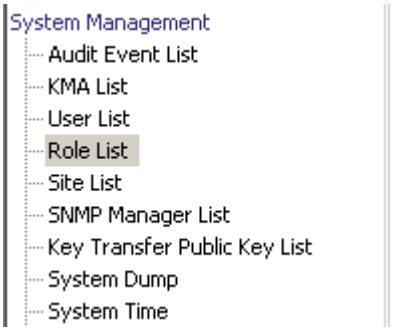
ユーザーを削除するには、次の手順を実行します。

1. 「Users List」画面で、削除するユーザーを選択して「**Delete**」ボタンをクリックします。次のように、選択したユーザーの削除を確認するダイアログボックスが表示されます。

2. 「**Yes**」ボタンをクリックして、ユーザーを削除します。現在選択しているユーザーが削除され、「User List」画面に戻ります。削除したユーザーは表示されなくなります。

「Role List」メニュー

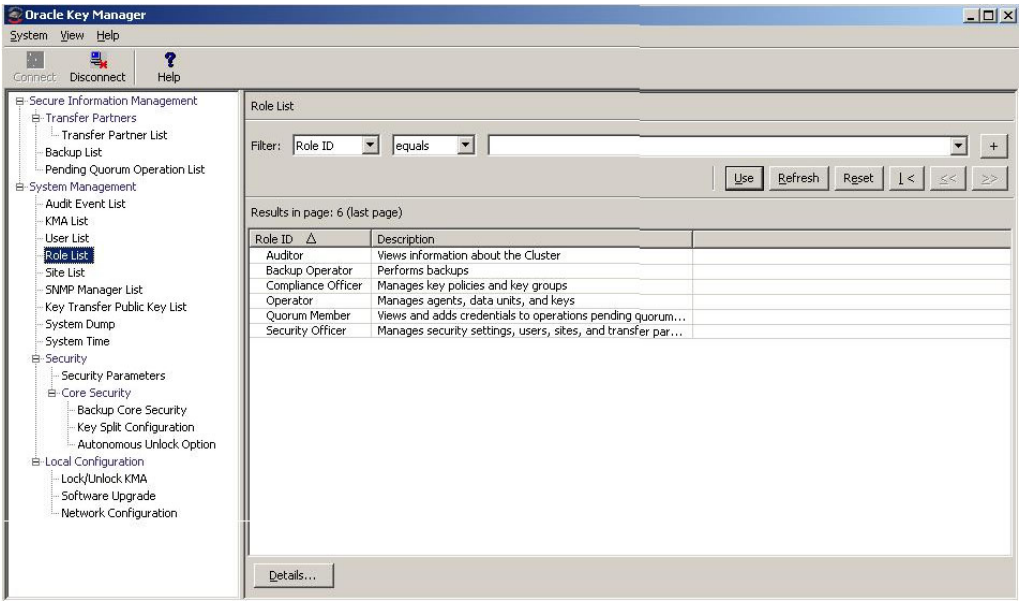
「Role List」メニューオプションを使用すると、ユーザーの役割を表示できます。役割とは、ユーザーが実行できるさまざまなシステム操作の、固定された論理グループを指します。1 人のユーザーに複数の役割を付与できます。



役割の表示

役割を表示するには、次の手順を実行します。

「System Management」メニューから、「**Role List**」を選択します。「Role List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで役割リストにフィルタを適用することもできます。

- Role ID
- 解説 .

表示されているリストにフィルタを適用するには、「Use」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- Role ID
- 説明

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- 空白
- 空白以外

フィルタ値 1 ボックス :

このフィールドに値を入力します。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Role ID

各セキュリティーの役割を識別する一意の識別子が表示されます。

説明

役割の説明が示されます。

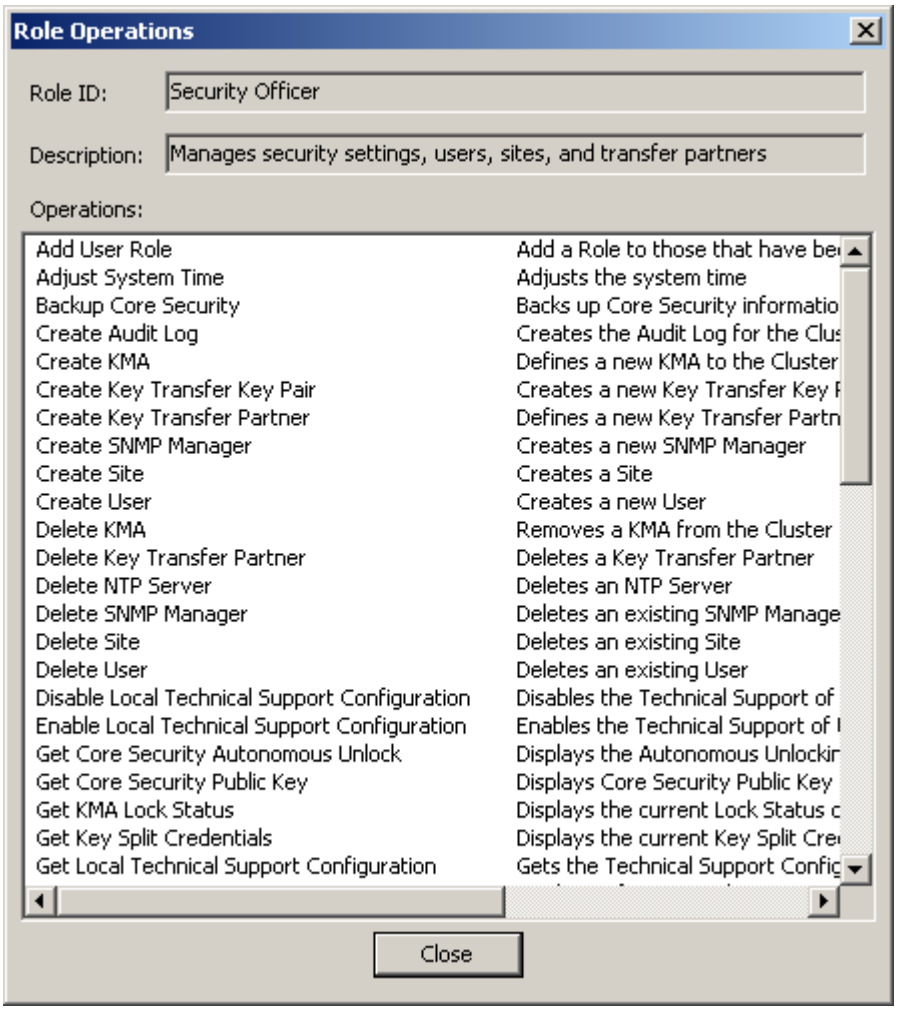
役割の詳細情報を表示する場合は、その役割エントリを強調表示して「**Details**」ボタンをクリックします。詳細については、151 ページの「役割の操作の表示」を参照してください。

役割の操作の表示

「Role Operations」ダイアログボックスを使用すると、役割とその役割で許可されている操作を表示できます。

特定の役割の操作を表示するには、次の手順を実行します。

1. 「Role List」画面で、役割を強調表示して「**Details**」ボタンをクリックします。「Role Operations」ダイアログボックスが表示され、選択した役割の操作が示されます。



2. このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。「Role List」画面に戻ります。

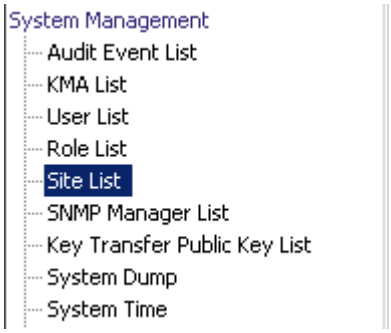
「Site List」メニュー

サイトとは、複数のエージェント (ホストと OKM クラスタ) の接続先となる、1 つ以上の KMA が存在する物理的な場所です。エージェントは、遠隔のサイトではなくローカルのサイトにある別の KMA に接続することによって、KMA の障害や負荷分散により効率的に対応できます。

「Site List」メニューオプションを使用すると、次の操作を行うことができます。

- サイトの表示
- サイトの作成
- サイトの情報の変更
- サイトの削除

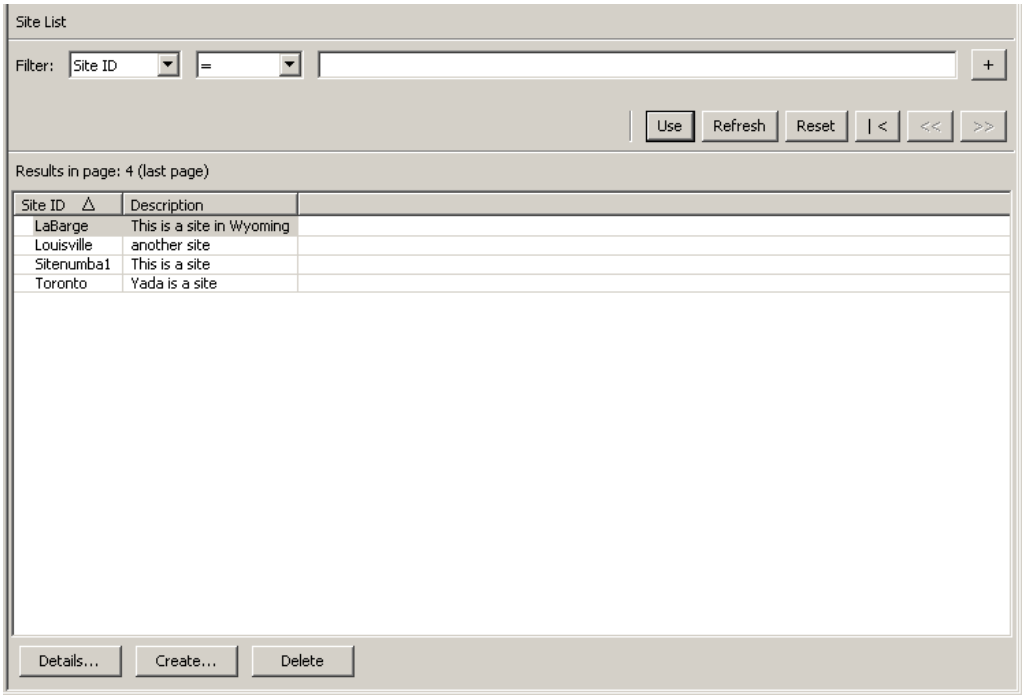
注 ー オペレータは、サイトの表示のみを行うことができます。セキュリティー責任者は、サイトを管理できます。



サイトの表示

サイトを表示するには、次の手順を実行します。

「System Management」メニューから、「**Site List**」を選択します。「Site List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでサイトリストにフィルタを適用することもできます。

- Site ID
- 解説。

表示されているサイトリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ：

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- Site ID
- 説明

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~

フィルタ値 1 ボックス :

このフィールドに値を入力します。

使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Site ID

サイトが一意に識別されます。

説明

サイトの説明が示されます。

サイトを作成するには、「Create」ボタンをクリックします。詳細については、156 ページの「サイトの作成」を参照してください。

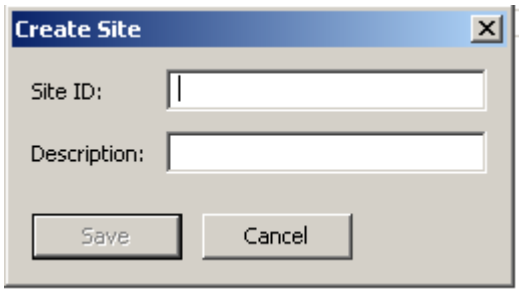
サイトの詳細情報を表示または変更する場合は、そのサイトを強調表示して「Details」ボタンをクリックします。詳細については、158 ページの「サイトの詳細の表示および変更」を参照してください。

選択したサイトを削除するには、「Delete」ボタンをクリックします。詳細については、159 ページの「サイトの削除」を参照してください。

サイトの作成

サイトを作成するには、次の手順を実行します。

1. 「Site List」画面で、「**Create**」ボタンをクリックします。「Create Site」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

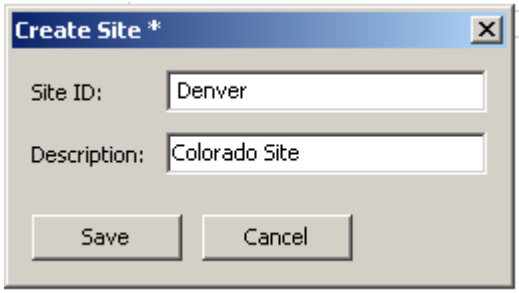
Site ID

サイトを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

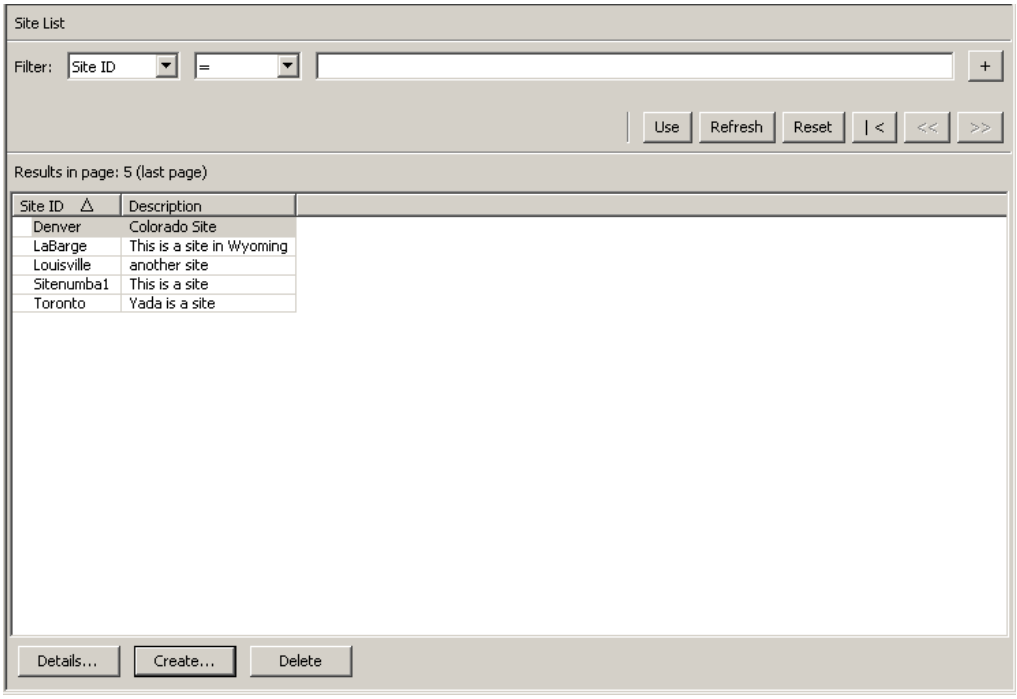
説明

サイトを一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

次に、値を入力したダイアログボックスの例を示します。



3. 「**Save**」ボタンをクリックします。新しいサイトが保存されてデータベースに格納され、「Site List」に表示されます。

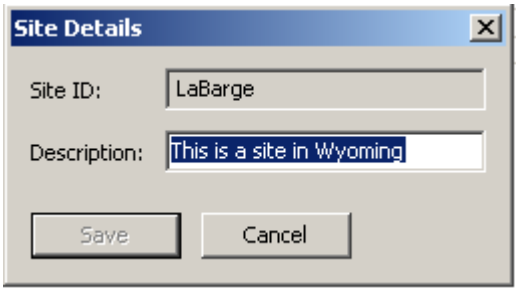

Site List
Filter:
Site ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 5 (last page)
Site ID
Description
Denver
Colorado Site
LaBarge
This is a site in Wyoming
Louisville
another site
Sitenumba1
This is a site
Toronto
Yada is a site
Details...
Create...
Delete

サイトの詳細の表示および変更

注 ー セキュリティー責任者以外のユーザーがサイトの詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

サイトの詳細を変更するには、次の手順を実行します。

1. 「Site List」画面で、「**Details**」ボタンをクリックします。「Site Details」ダイアログボックスが表示されます。



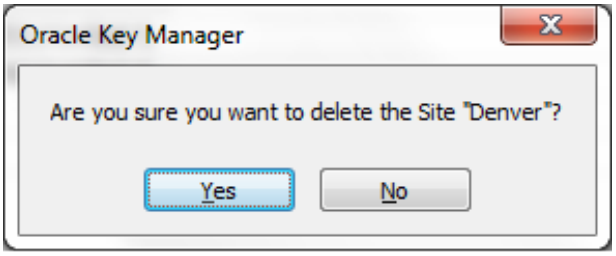
2. 「Description」フィールドを変更し、「**Save**」ボタンをクリックします。サイトの詳細が変更され、データベースに格納されます。

サイトの削除

注 ー サイトが使用されている場合、つまりサイトにエージェントまたは KMA が指定されている場合は、サイトを削除する前に、これらのエージェントや KMA を削除するか、または別のサイトに変更する必要があります。

サイトを削除するには、次の手順を実行します。

1. 「Site List」画面で、削除するサイトを強調表示して「**Delete**」ボタンをクリックします。次のように、操作を確認するダイアログボックスが表示されます。



2. 「**Yes**」ボタンをクリックして、サイトを削除します。現在選択しているサイトが削除され、「Site List」画面に戻ります。

「SNMP Manager List」メニュー

SNMP マネージャーを表示、作成、および変更するには、ここで説明するメニューを使用します。

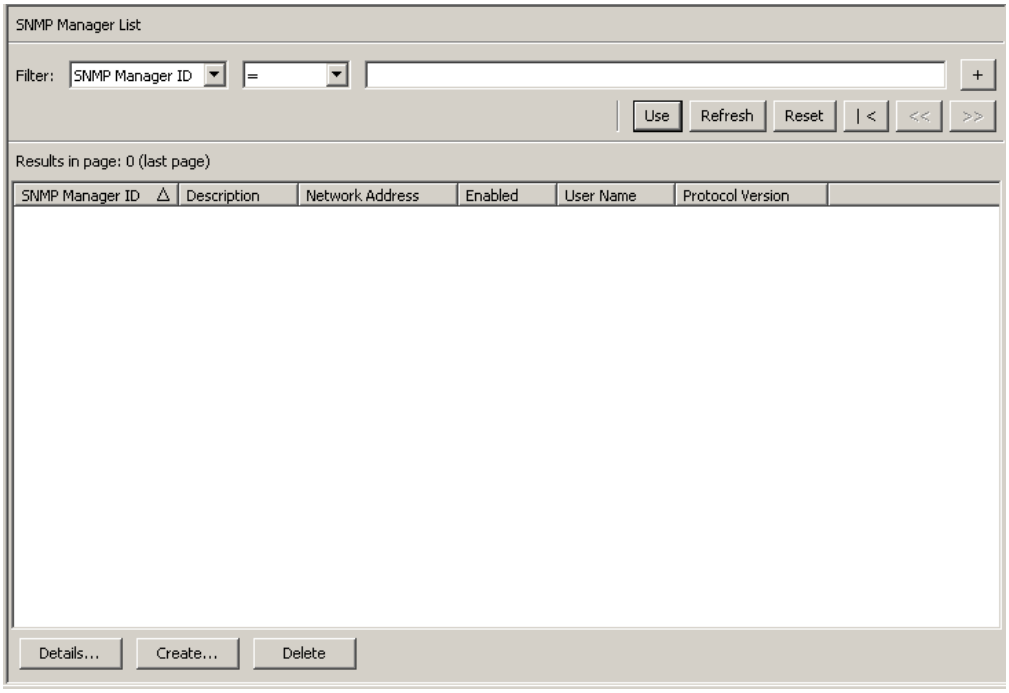
また、各自のネットワークで SNMP エージェントを設定し、OKM Manager の GUI で SNMP マネージャーを定義したユーザーの SNMP 情報を生成できます。OKM Manager の GUI で 1 つ以上の SNMP マネージャーを定義すると、KMA がその SNMP マネージャーの IP アドレスに SNMP インフォームを送信します。

SNMP インフォームパケットで KMA が送信する情報については、407 ページの「SNMP 管理情報ベース (MIB) データ」を参照してください。

KMA の SNMP マネージャーの表示

SNMP マネージャーを表示するには、次の手順を実行します。

「System Management」メニューから、「**SNMP Manager List**」を選択します。「SNMP Manager List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで SNMP マネージャーリストにフィルタを適用することもできます。

- SNMP Manager ID
- 説明
- ネットワークアドレス
- 有効
- ユーザー名。

表示されている SNMP マネージャーリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- SNMP Manager ID
- 説明
- ネットワークアドレス
- 有効
- ユーザー名 .

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値 1 ボックス :

このフィールドに値を入力します。

使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

SNMP Manager ID

ユーザーが定義した SNMP マネージャーの一意の識別子が表示されます。

説明

SNMP マネージャーの説明が表示されます。このフィールドは省略可能です。

ネットワークアドレス

SNMP トラップの送信時に使用するネットワークアドレスが表示されます。

有効

SNMP マネージャーが使用可能かどうかが示されます。

ユーザー名

この SNMP マネージャーに対してセキュリティー保護された信頼できる SNMPv3 接続を確立するときに使用されたユーザー名が表示されます。

Protocol Version

SNMP プロトコルのバージョンを示します。SNMPv3 (バージョン 3) または SNMPv2 (バージョン 2) のどちらかです。

SNMP プロトコルバージョン 3 (SNMPv3) は、ユーザー名とパスフレーズを使用した認証をサポートします。SNMP プロトコルバージョン 2 (SNMPv2) は、認証をサポートせず、ユーザー名とパスフレーズを使用しません。SNMPv3 または SNMPv2 のどちらかを使用するように SNMP マネージャーを設定できます。OKM クラスタの複製バージョンが現在 10 またはそれ以下に設定されている場合、KMA は、SNMPv2 を使用するように設定された SNMP マネージャーに SNMP インフォームを送信しません。

新しい SNMP マネージャーを作成するには、「**Create**」ボタンをクリックします。詳細は、「新しい SNMP マネージャーの作成」を参照してください。

SNMP マネージャーの詳細情報を表示または変更する場合は、そのエントリを強調表示して「**Details**」ボタンをクリックします。詳細については、167 ページの「SNMP マネージャーの詳細の表示および変更」を参照してください。

選択した SNMP マネージャーを削除するには、「**Delete**」ボタンをクリックします。詳細については、168 ページの「SNMP マネージャーの削除」を参照してください。

新しい SNMP マネージャーの作成

注 –

SNMP プロトコルバージョン 3 を使用するように SNMP エージェントが設定されている場合は、OKM クラスタに SNMP マネージャーを作成する前に、必ず SNMP プロトコルバージョン 3 のユーザーを作成しておいてください。この SNMP ユーザーは、認証プロトコルには (MD5 ではなく) SHA を、プライバシープロトコルには DES を使用する必要があります。SNMP バージョン 3 ユーザーの作成については、お使いの SNMP エージェントのドキュメントを参照してください。

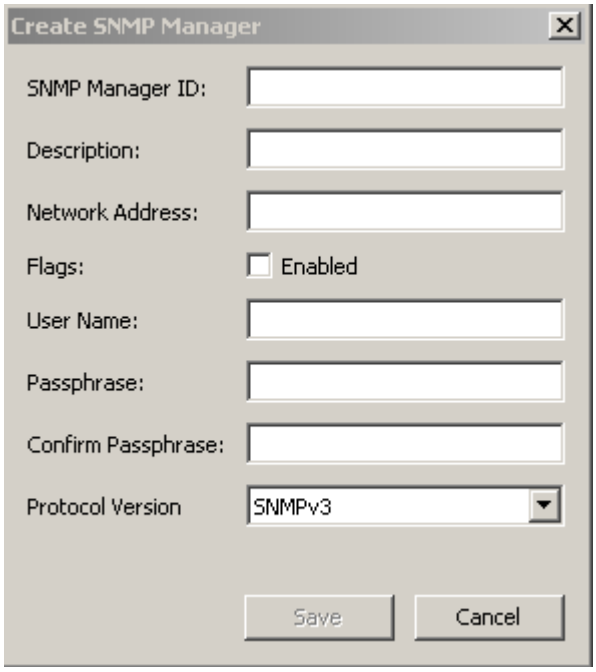
また、SNMP ユーザーがパスフレーズを持つ場合、KMA はその SNMP ユーザーの認証パスフレーズと暗号化パスフレーズの両方にこのパスフレーズを使用します。したがって、SNMP エージェントで、この SNMP ユーザーについてこれらのパスフレーズが同じ値である必要があります。SNMP ユーザーがパスフレーズを持たない場合、KMA は SNMP インフォームを SNMP エージェントに送信するときに「noAuthNoPriv」のセキュリティーレベルを使用します。

SNMP プロトコルバージョン 2 を使用するように SNMP エージェントが設定されている場合、認証プロトコルの設定または SNMP ユーザーの作成は必要ありません。現時点で、OKM はバージョン 2 の「public」コミュニティーのみをサポートします。

SNMP ユーザーの作成については、お使いの SNMP エージェントのドキュメントを参照してください。たとえば、Solaris システムでのシステム管理エージェントの設定については、『Solaris System Management Agent Administration Guide』(http://docs.sun.com/app/docs/doc/817-3000) を参照してください。また、Net-SNMP 全般についての詳細は、http://www.net-snmp.org/FAQ.html を参照してください。

1. 「SNMP Managers List」画面で、「**Create**」ボタンをクリックします。

   「Create SNMP Manager」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

SNMP Manager ID

SNMP マネージャーを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

説明

SNMP マネージャーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

ネットワークアドレス

SNMP マネージャーのネットワークアドレスを入力します。

Flags - Enabled

このチェックボックスの選択によって、SNMP を使用可能にするかどうかを示します。

ユーザー名

SNMP マネージャーの認証に使用するユーザー名を入力します。

パスフレーズ

SNMP マネージャーの認証に使用するパスフレーズを入力します。

Confirm Passphrase

「Passphrase」フィールドに入力したパスフレーズと同じ値を入力します。

Protocol Version

この SNMP マネージャーで使用する SNMP プロトコルバージョンを選択します。値 SNMPV3 は、SNMP プロトコルバージョン 3 を使用することを意味します。値 SNMPV2 は、SNMP プロトコルバージョン 2 を使用することを意味します。

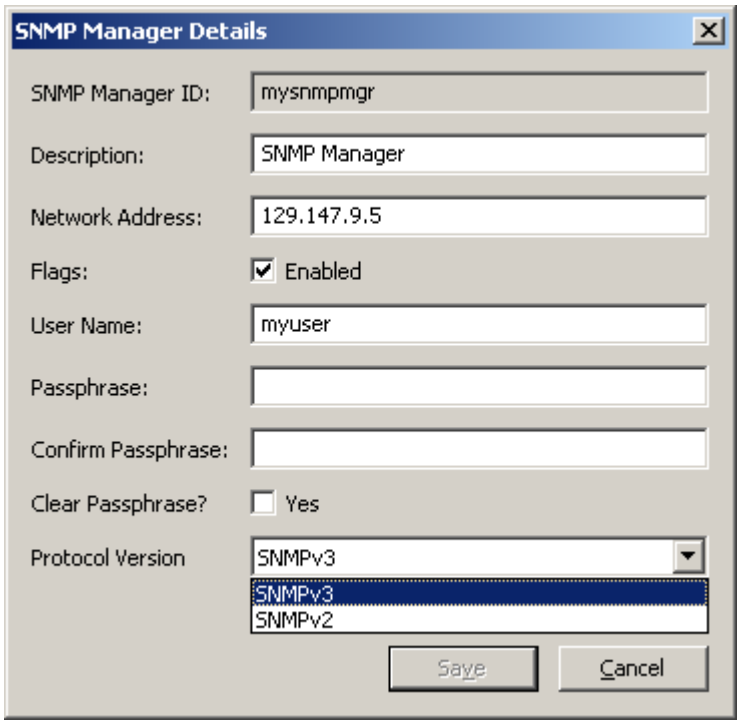
SNMP プロトコルバージョン 3 (SNMPv3) は、ユーザー名とパスフレーズを使用した認証をサポートします。SNMP プロトコルバージョン 2 (SNMPv2) は、認証をサポートせず、ユーザー名とパスフレーズを使用しません。SNMPv3 または SNMPv2 のどちらかを使用するように SNMP マネージャーを設定できます。OKM クラスタの複製バージョンが現在 10 またはそれ以下に設定されている場合、KMA は、SNMPv2 を使用するように設定された SNMP マネージャーに SNMP インフォームを送信しません。

3. 終了したら、「**Save**」ボタンをクリックして情報を保存します。新しい SNMP マネージャーエントリと、それに関連するプロファイルがデータベースに格納されます。

SNMP マネージャーの詳細の表示および変更

SNMP マネージャーの詳細を表示または変更するには、次の手順を実行します。

1. 「SNMP Managers List」画面で、詳細情報を表示する SNMP マネージャーエントリをダブルクリックし、「**Details**」ボタンをクリックします。「SNMP Manager Details」ダイアログボックスが表示されます。



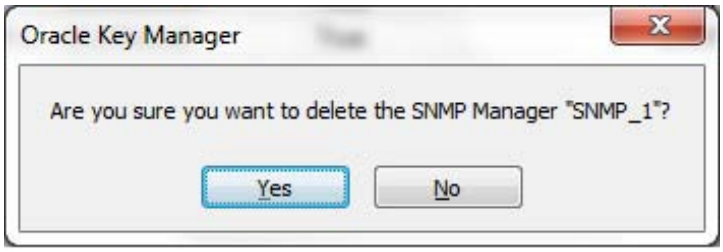
2. 必要に応じて、パラメータを変更します。
3. 終了したら、「**Save**」ボタンをクリックして変更内容を保存します。

注 – SNMP マネージャーの詳細を変更するたびに、パスフレーズを再指定する必要があります。

SNMP マネージャーの削除

SNMP マネージャーを削除するには、次の手順を実行します。

1. 「SNMP Managers List」画面で、削除する SNMP マネージャーを強調表示して「**Delete**」ボタンをクリックします。SNMP マネージャーの削除を確認するダイアログボックスが表示されます。



2. 「**Yes**」ボタンをクリックして、SNMP マネージャーを削除します。現在選択している SNMP マネージャーが削除され、「SNMP Manager List」画面に戻ります。

鍵転送

概要

鍵転送は鍵共有とも呼ばれ、鍵と関連データユニットをパートナー間で安全に交換することを可能にします。また、暗号化された媒体を交換するためにも必要です。この処理では、転送の送信側と受信側の両方が公開鍵と非公開鍵のペアを設定して、相手側に公開鍵を提供する必要があります。

送信側と受信側はそれぞれ、相手側の公開鍵を自身の OKM クラスタに入力します。この初期設定が完了すると、送信側は鍵のエクスポートを使用して転送ファイルを生成します。このファイルが送信側から受信側に送信されます。次に、受信側が鍵のインポートを使用して、鍵とそれに関連付けられたデータユニットを受信側の OKM クラスタにインポートします。

転送ファイルは、送信側の非公開鍵を使用して署名され、受信側の公開鍵を使用して暗号化されます。これにより、受信側のみが自身の非公開鍵を使用して転送ファイルを復号化できます。受信側は、送信側の公開鍵を使用して、ファイルが実際に想定した送信側によって作成されたファイルであることを確認できます。

鍵転送パートナー機能

鍵転送パートナー機能を使用すると、OKM クラスタ間で鍵を移動できます。通常、会社間でテープを交換する場合、または多数のサイトに対処するために社内に複数のクラスタが構成されている場合に、この機能を使用できます。

鍵転送処理では、次の手順を実行します。

- 各 OKM クラスタで、別のクラスタを転送パートナーとして設定します。通常、この設定は 1 回だけ行います。
- ユーザーは、一方の OKM クラスタから鍵をエクスポートし、もう一方のクラスタにその鍵をインポートします。この手順は、何回でも実行できます。

鍵転送処理

OKM 内では、多数のタスクを特定の順序で実行する必要があります。これらのタスクには複数のユーザー役割が関連しているため、実際の手順については、このマニュアルの複数の章で説明します。

鍵転送パートナーの設定

鍵を移動するには、鍵の移動に関与する両方の OKM クラスタに鍵転送パートナーを設定する必要があります。

次の手順では、「C1」は 1 つめの OKM クラスタ、「C2」は 2 つめの OKM クラスタを指しています。

C1 管理者 (セキュリティー責任者の役割):

1. C1 (ユーザーのクラスタ) の公開鍵情報を取得します。この操作を行うには、「Key Transfer Public Key List」メニューに移動します。189 ページの「「Key Transfer Public Key List」の表示」および 192 ページの「鍵転送用公開鍵の詳細の表示」を参照してください。
2. 公開鍵 ID と公開鍵を電子メールまたはその他の合意済みの通信形式にカット & ペーストします。この情報を C2 管理者に送信します。

   注 ー C2 がこの情報を受信したとき、その情報は実際に C1 から送信されたものであると確信できるように、通信方法は十分にセキュリティー保護されている必要があります。情報が送信中に改ざんされることを防ぐために、フィンガープリントという機構があります。

C2 管理者 (セキュリティー責任者の役割):

3. C2 管理者 : 「Transfer Partner List」メニューにアクセスし、C1 からの公開鍵情報を OKM クラスタに入力します。175 ページの「「Transfer Partner List」メニュー」を参照してください。
4. 「**Create...**」ボタンをクリックします。転送パートナーの名前、説明、および連絡先情報を入力します。このパートナーとの間で行う処理を設定します。179 ページの「転送パートナーの作成」を参照してください。
5. 「Public Keys」タブを選択します。C1 から提供された情報から、公開鍵 ID と公開鍵を入力します。

   公開鍵を入力すると、システムによってフィンガープリントが計算されます。C1 管理者と C2 管理者との間の通信には、鍵自体の転送に使用したものとは別の機構を使用することをお勧めします。

   両方の管理者は、各自の OKM で、フィンガープリントが一致することを確認する必要があります。フィンガープリントが一致しない場合は、転送中に鍵が壊れたか、または変更されたことを示します。

6. フィンガープリントが一致した場合は、「**Save**」をクリックします。システムから定足数の入力が求められます。定足数が求められるのは、この手順で使用可能にする鍵のエクスポート操作が、OKM クラスタから有効な鍵を抽出するために使用される可能性があるためです。これで、C1 は C2 OKM クラスタ内で転送パートナーとして設定されました。

C2 管理者 (セキュリティー責任者の役割):

7. 今度は C2 OKM クラスタで、手順 1 と手順 2 を繰り返します。

C1 管理者 (セキュリティー責任者の役割):

8. 手順 3 ～手順 6 を繰り返して、C2 の公開鍵を C1 に追加します。

C1 管理者 (コンプライアンス責任者の役割):

9. C1 では、C2 に送信できる鍵グループを設定する必要があります。273 ページの「鍵グループ割り当ての表示」を参照してください。

C2 管理者 (コンプライアンス責任者の役割):

10. C2 では、C1 から鍵を受信できる鍵グループを設定する必要があります。273 ページの「鍵グループ割り当ての表示」を参照してください。

11. 必要な転送パートナーを選択します。

12. 許可されていない鍵グループを 1 つ以上選択し、「Move to  」ボタンをクリックして鍵グループリストに追加します。274 ページの「転送パートナーへの鍵グループの追加」を参照してください。

鍵のエクスポートおよびインポート

鍵をエクスポートする前に、鍵が次の基準をすべて満たしている必要があります。基準を満たさない鍵は、オペレータが鍵のエクスポート要求を実行してもエクスポートされません。

- 「Allow Export From」フラグが「True」に設定された鍵ポリシーと関連付けられた鍵グループに鍵が属している必要があります。314 ページの「データユニットの詳細の表示および変更」および 253 ページの「鍵グループの表示」を参照してください。

  フラグを設定するには、248 ページの「鍵ポリシーの表示および変更」を参照してください。

- 宛先の鍵転送パートナーの「Enabled and Allow Export To」フラグが「True」に設定されている必要があります。183 ページの「転送パートナーの詳細の表示および変更」を参照してください。

  フラグを設定するには、248 ページの「鍵ポリシーの表示および変更」を参照してください。

- 宛先の鍵転送パートナーが、選択された鍵の鍵グループと関連付けられている必要があります。274 ページの「転送パートナーへの鍵グループの追加」を参照してください。

- 鍵の状態は「Protect and Process」、「Process Only」、「Deactivated」、または「Compromised」である必要があります。314 ページの「データユニットの詳細の表示および変更」を参照してください。

さらに、宛先転送パートナー (175 ページの「「Transfer Partner List」メニュー」を参照) の、次に示す**エクスポート形式**設定が一致する必要があります。

- 鍵がインポートされる KMA の**ソフトウェアバージョン** (322 ページの「ソフトウェアアップグレードのアップロードおよび適用」を参照)
- 鍵がエクスポートおよびインポートされる OKM クラスタの「FIPS Mode Only」セキュリティーパラメータ値 (207 ページの「セキュリティーパラメータの取り出し」を参照)

表 5-1 に、これらの設定間の関係をまとめます。

表 5-1 エクスポート形式設定

ソフトウェアバージョン - インポート側 KMA	FIPS Mode Only - エクスポート側 OKM クラスタ	FIPS Mode Only - インポート側 OKM クラスタ	エクスポート形式
2.0.2 以前	Off	N/A	v2.0 または Default
2.0.2 以前	点灯	N/A	v2.0
2.1 以降	Off	Off	v2.0 または Default
2.1 以降	点灯	Off	v2.0
2.1 以降	Off	点灯	v2.1 (FIPS)
2.1 以降	点灯	点灯	v2.1 (FIPS) またはデフォルト

次の手順は、ある OKM クラスタから別のクラスタに対して、鍵のエクスポートおよびインポートを行う場合に使用します。この手順は、何回でも実行できます。

次の手順では、「C1」は 1 つめの OKM クラスタ、「C2」は 2 つめの OKM クラスタを指しています。この手順では、C2 で鍵をエクスポートし、その鍵を C1 にインポートできるようにする方法について説明します。

C2 管理者 (オペレータの役割):

1. 鍵を交換するには、「Data Unit List」画面に移動します。310 ページの「データユニットの表示」を参照してください。
2. C2 から C1 に送信するデータユニット (テープ) を 1 つ以上選択します。外部タグは、テープ上のバーコードです。

   選択したデータユニットと関連付けられた鍵は、「`Allow Export From`」フラグが「True」に設定された鍵ポリシーと関連付けられた鍵グループに属している必要があります。さらに、これらの鍵はアクティブ化される必要があり (アクティブ化日付が空でない)、破棄されてはいけません (破棄日付が空)。314 ページの「データユニットの詳細の表示および変更」を参照してください。
3. 「**Export Keys**」ボタンをクリックし、ダイアログボックスを表示します。
4. 宛先の転送パートナーを選択し、必要に応じて鍵のエクスポートファイル名を選択して「**Start**」をクリックします。転送ファイルが作成されます。

   C1 へのエクスポートが許可されている鍵グループに属する鍵のみがエクスポートされます。

   選択した宛先転送パートナーが、これらの鍵が属する鍵グループに割り当てられている必要があります。276 ページの「「Transfer Partner Assignment to Key Groups」メニュー」を参照してください。
5. 電子メールまたは別の合意済みの通信形式、またはファイルを移動するメカニズムを使用して、転送ファイルを C1 管理者に送信します。

C1 管理者 (オペレータの役割):

6. 「Import Keys」画面を選択します。307 ページの「「Import Keys」メニュー」を参照してください。
7. 鍵のインポート先になる宛先の鍵グループ、鍵をエクスポートした送信側転送パートナー (この場合は C2)、および鍵転送のファイル名を指定します。選択する鍵グループは、C2 から鍵を受信するように設定された鍵グループである必要があります。

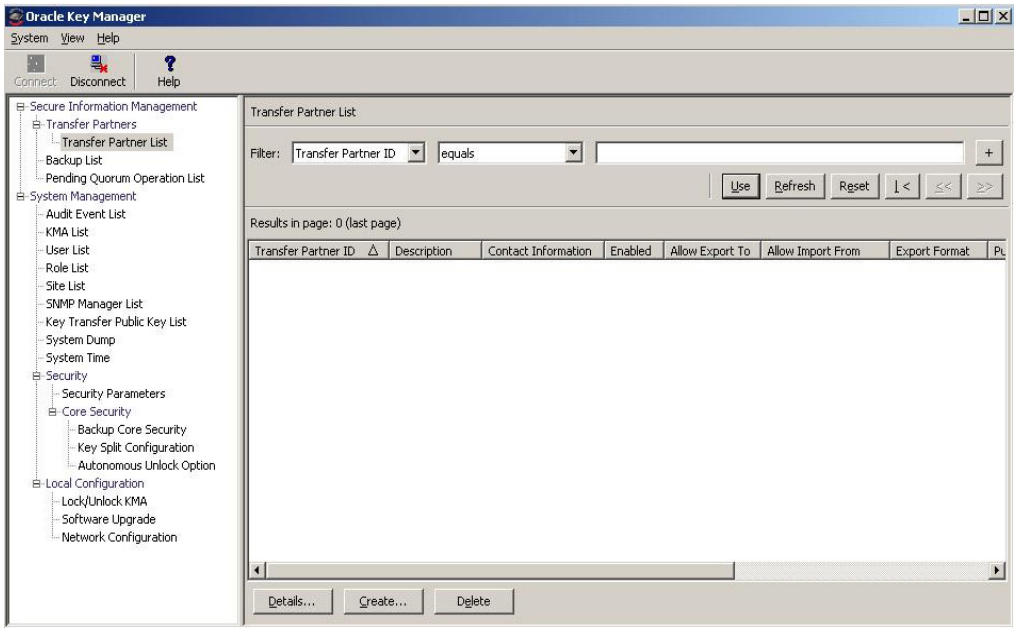
   つまり、選択する鍵グループと関連付けられた鍵ポリシーの「`Allow Import To`」フラグが「True」に設定されている必要があります。また、選択した転送パートナーの「`Enabled`」および「`Allow Import From`」フラグが「True」に設定され、そのエクスポート形式の値が先の説明のとおりに設定されている必要があります。選択した転送パートナーが、選択する鍵グループに割り当てられている必要があります。276 ページの「「Transfer Partner Assignment to Key Groups」メニュー」を参照してください。
8. 「Start」をクリックします。

「Transfer Partners」メニュー

鍵転送パートナー機能を使用すると、OKM クラスタ間で鍵を移動できます。

「Transfer Partner List」メニュー

「Secure Information Management」メニューから、「**Transfer Partner List**」を選択します。



データベース全体をスクロールするか、次のいずれかのキーで転送パートナーリストにフィルタを適用することもできます。

- Transfer Partner ID
- 説明
- 連絡先情報
- 有効
- Allow Export To
- Allow Import From

表示されている転送パートナーリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ：

表示されている公開鍵のリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタの条件を満たす転送パートナーのみが表示されます。

フィルタ属性コンボボックス :

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。取り得る値は次のとおりです。

- Transfer Partner ID
- 説明
- 連絡先情報
- 有効
- Allow Export To
- Allow Import From

フィルタ演算子コンボボックス :

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス :

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用 :

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Transfer Partner ID:

各転送パートナーを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

解説 :

転送パートナーについて説明します。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

連絡先情報 :

転送パートナーの連絡先情報が表示されます。この属性でソートするには、この列名をクリックします。

有効 :

転送パートナーに鍵の共有が許可されているかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、転送パートナーは鍵を共有できません。この属性でソートするには、この列名をクリックします。

Allow Export To:

転送パートナーに鍵のエクスポートが許可されているかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、転送パートナーは鍵をエクスポートできません。この属性でソートするには、この列名をクリックします。

Allow Import From:

この転送パートナーから鍵をインポートできるかどうかが示されます。True または False の値を取ります。このフィールドが False の場合、この転送パートナーから鍵をインポートできません。この属性でソートするには、この列名をクリックします。

Export Format:

鍵をラップできるかどうかを示します (ラップ鍵は、LAN 上の媒体鍵とトークンを暗号化します)。

「Export Format」列で、値「v2.0」は、鍵をエクスポートするときにこの転送パートナーが鍵をラップしないことを意味します。

値「v2.1 (FIPS)」は、鍵をエクスポートするときにこの転送パートナーが鍵をラップすることを意味します。

値「N/A」は、接続された KMA が 2.0.x OKM ソフトウェアを実行しているため、ユーザーがこの設定を選択できないことを意味します。

> **注 ー** KMS 2.0 を実行しているクラスタと鍵を交換するには、「Export Format」の値が「v2.0」である転送パートナーをセキュリティー責任者が作成する必要があります。

詳細は、207 ページの「セキュリティーパラメータの取り出し」の「FIPS Mode Only」パラメータを参照してください。

Public Key ID

各公開鍵を識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

Public Key Fingerprint

公開鍵のフィンガープリント (ハッシュ値) が表示されます。

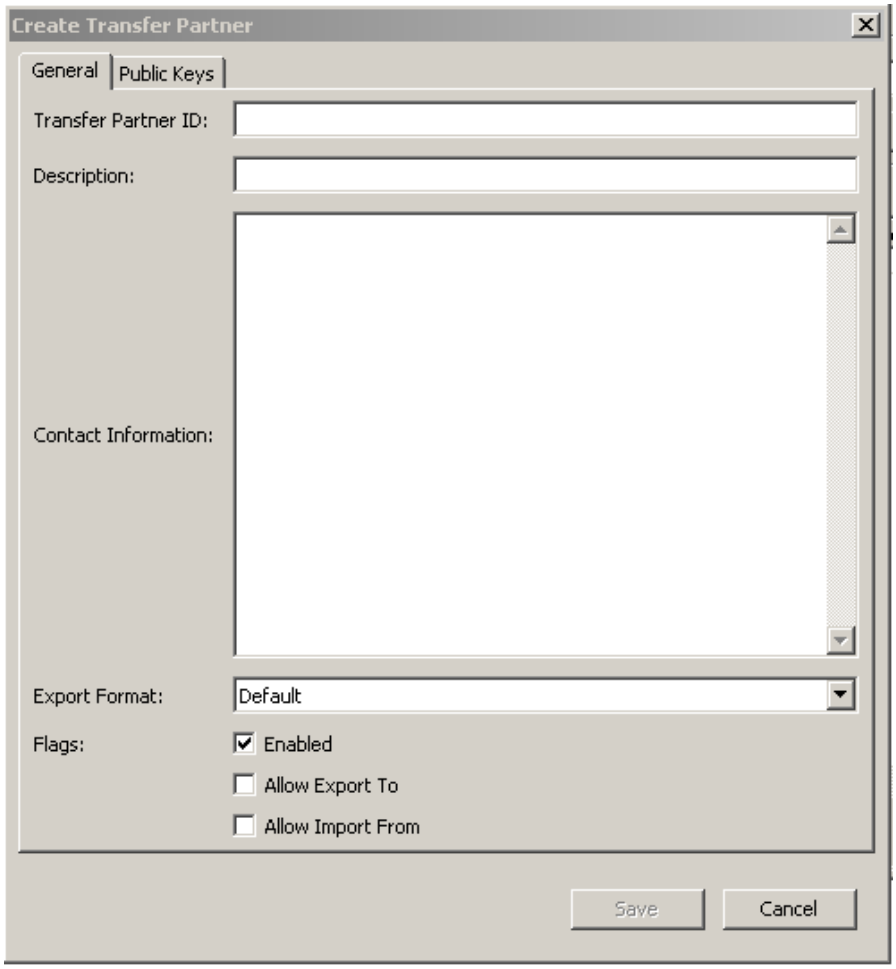
Entry Date

公開鍵が OKM クラスタに格納された日付が表示されます。

転送パートナーの作成

転送パートナーを作成するには、次の手順を実行します。

1. 「Transfer Partner List」画面で、「**Create**」ボタンをクリックします。「Create Transfer Partner」ダイアログボックスが表示され、「General」タブがアクティブになっています。



2. 次のパラメータを設定します。

「General」タブ

Transfer Partner ID

転送パートナーが一意に識別されます。

説明

転送パートナーを一意に説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

連絡先情報

転送パートナーの連絡先情報を識別する値を入力します。このフィールドは、空白のままにすることができます。

エクスポート形式

「Default」、「v2.0」、「v2.1 (FIPS)」のいずれかを選択してエクスポート形式を決定します。

値「v2.0」は、鍵をエクスポートするときにこの転送パートナーが鍵をラップしないことを意味します。

値「v2.1 (FIPS)」は、鍵をエクスポートするときにこの転送パートナーが鍵をラップすることを意味します。

値「Default」は、この転送パートナー用の鍵転送ファイルをエクスポートするとき、「FIPS Mode Only」セキュリティーパラメータの設定によって形式が決まることを意味します (207 ページの「セキュリティーパラメータの取り出し」を参照)。

「FIPS Mode Only」が「Off」の場合、形式は「v2.0」になります。「FIPS Mode Only」が「On」の場合、形式は「v2.1 (FIPS)」になります。

> **注 ー** 転送パートナーのエクスポート形式を「Default」に設定することの利点は、転送パートナーのエクスポート形式設定を直接編集 (この場合、変更を認証するために定足数が必要) しなくても、「FIPS Mode Only」セキュリティーパラメータを変更するだけで転送パートナーの転送ファイルの形式を変更できることです。

Flags - Enabled

この転送パートナーに鍵の共有を許可するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、転送パートナーは鍵を共有できません。

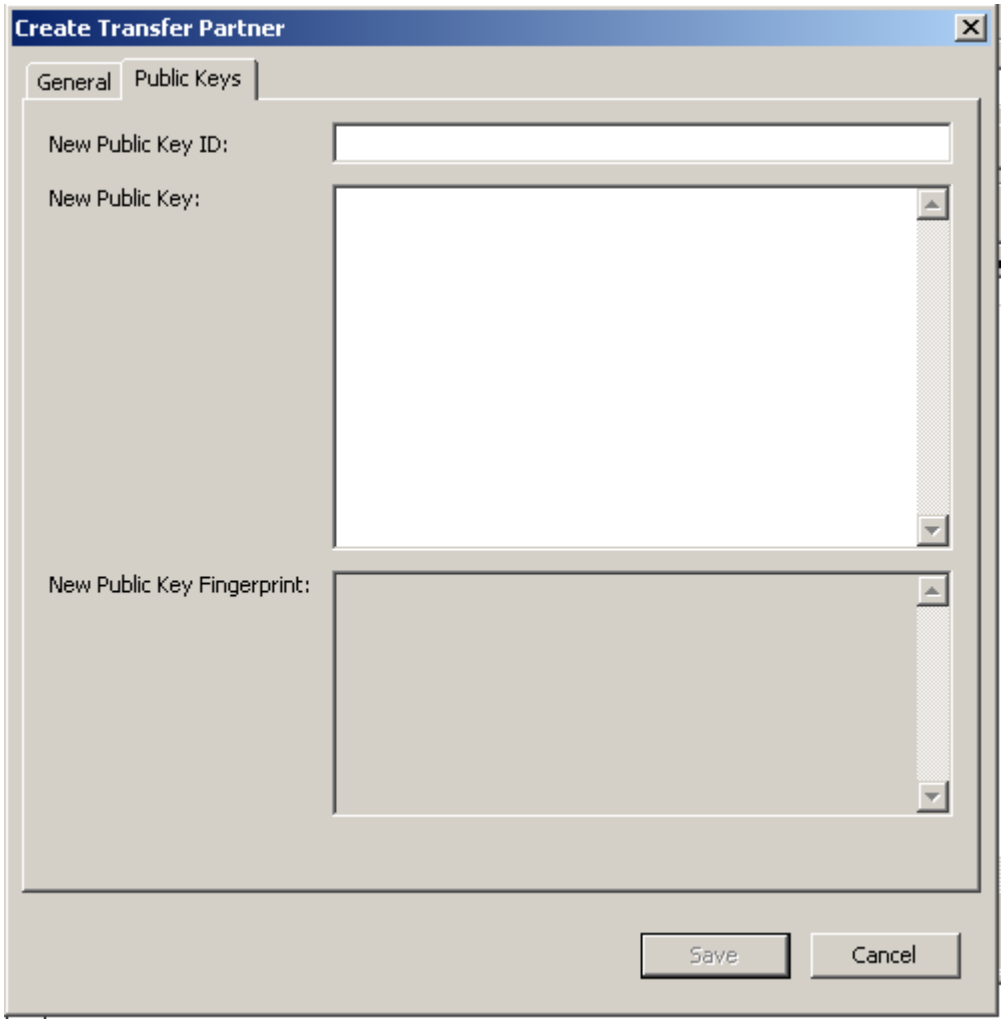
Allow Export To

転送パートナーへの鍵のエクスポートを許可するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、転送パートナーは鍵のエクスポート操作を実行できません。

Allow Import From

この転送パートナーから鍵をインポートできるように指定するには、このボックスにチェックマークを付けます。このフィールドが選択されていない場合、この転送パートナーから鍵をインポートできません。

3. 「Public Keys」タブを開きます。



「Public Keys」タブ

New Public Key ID

転送パートナーから提供された公開鍵 ID を入力します。

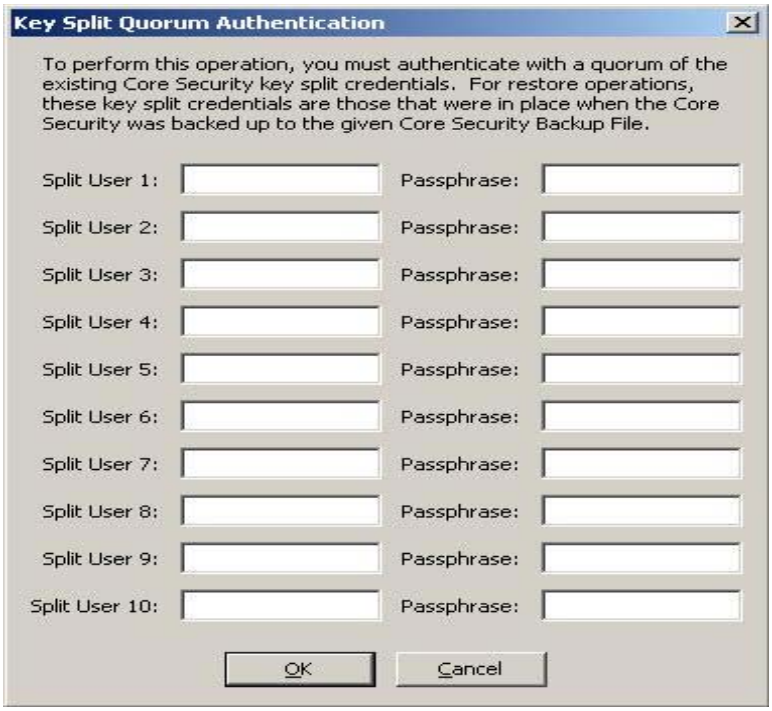
New Public Key

転送パートナーから提供された公開鍵を入力します。

New Public Key Fingerprint

この読み取り専用のフィールドには、新しい公開鍵のフィンガープリント (ハッシュ値) が表示されます。このフィンガープリントをパートナーと照合して、伝送中に偶然または故意に公開鍵が改ざんされていないことを確認します。

4. 終了したら、「**Save**」ボタンをクリックします。
5. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

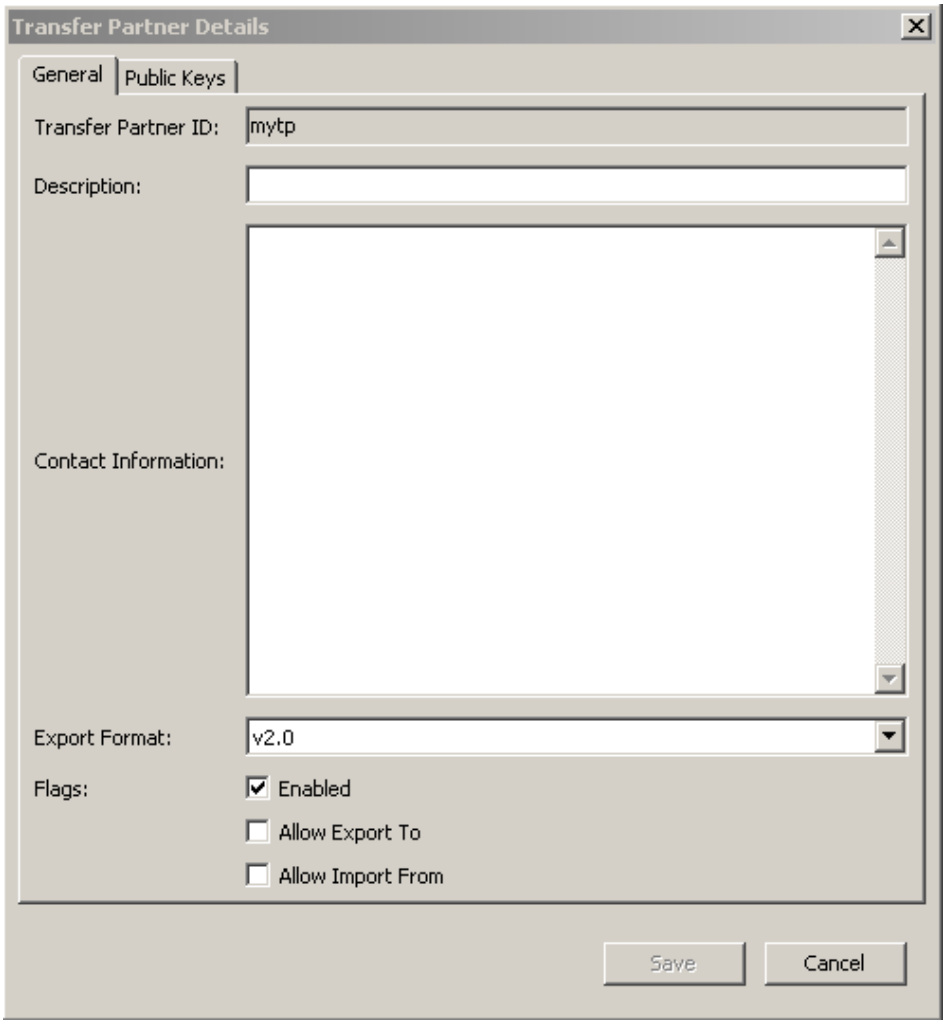
複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

転送パートナーの詳細の表示および変更

「Transfer Partner Details」ダイアログボックスを使用すると、特定の転送パートナーに関する詳細情報を表示できます。

詳細を表示するには、次の手順を実行します。

1. 「Transfer Partner List」画面で、転送パートナー ID を強調表示して「**Details**」ボタンをクリックします。「Transfer Partner Details」ダイアログボックスが表示されます。



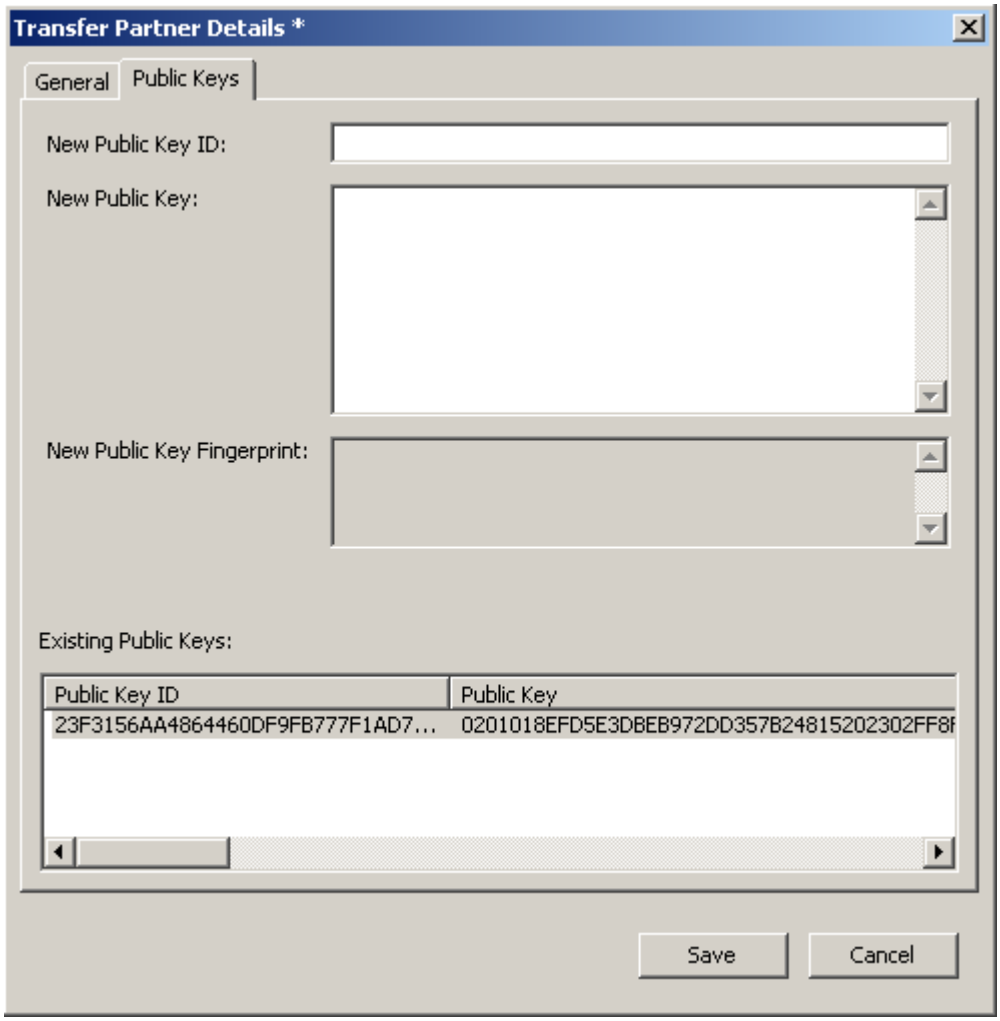
「General」タブ

2. 「General」タブでは、次のフィールドを変更できます。

- 説明
- 連絡先情報
- エクスポート形式
- Flags - Enabled
- Allow Export To
- Allow Import From

「Transfer Partner ID」フィールドは、読み取り専用です。

3. 終了したら、「**Save**」ボタンをクリックします。データベース内の転送パートナーレコードが変更されます。
4. 「Public Keys」タブを開きます。



「Public Keys」タブ

5. 「Public Keys」タブでは、次のフィールドを変更できます。

New Public Key ID

転送パートナーから提供された新しい公開鍵 ID を入力します。

New Public Key

転送パートナーから提供された新しい公開鍵を入力します。

New Public Key Fingerprint

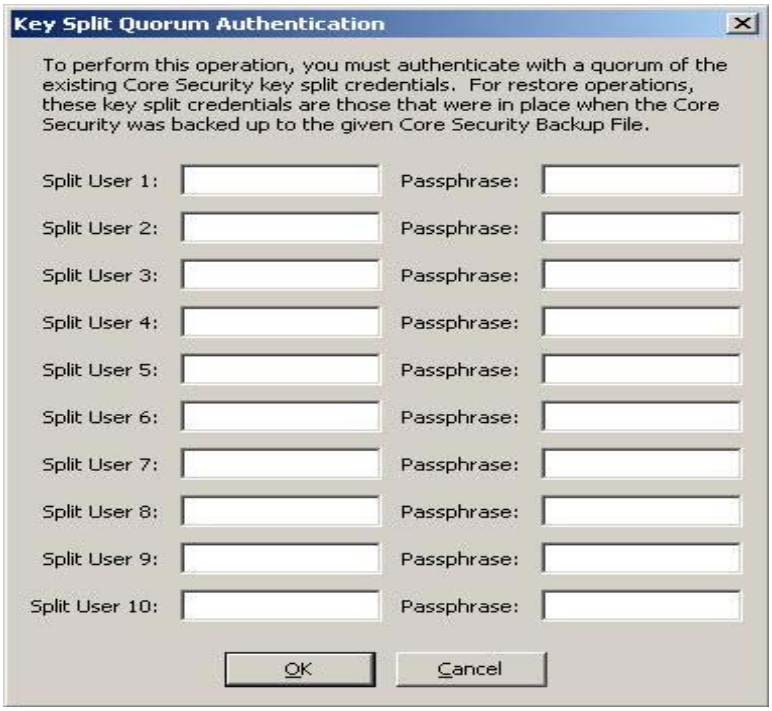
この読み取り専用のフィールドには、新しい公開鍵のフィンガープリント (ハッシュ値) が表示されます。この鍵を送信側転送パートナーに確認します。

Existing Public Keys

このリストには、この転送パートナーと関連付けられた公開鍵が表示されます。

6. 終了したら、「**Save**」ボタンをクリックします。

7. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

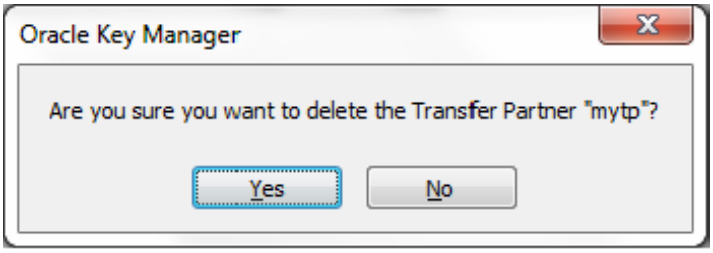
複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

転送パートナーの削除

このオプションを使用すると、セキュリティー責任者は、転送パートナーを削除できます。

転送パートナーを削除するには、次の手順を実行します。

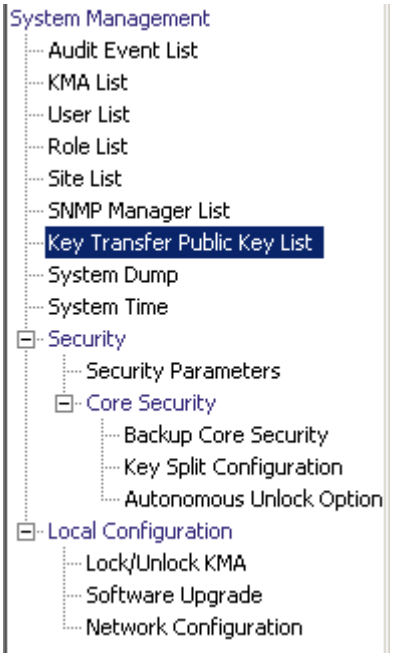
1. 「Transfer Partner List」画面で、削除する転送パートナー ID を強調表示して「**Delete**」ボタンをクリックします。転送パートナーの削除を確認するダイアログボックスが表示されます。



2. 「**Yes**」ボタンをクリックして、転送パートナーを削除します。現在選択している転送パートナーが削除され、「Transfer Partner List」画面に戻ります。

「Key Transfer Public Key List」メニュー

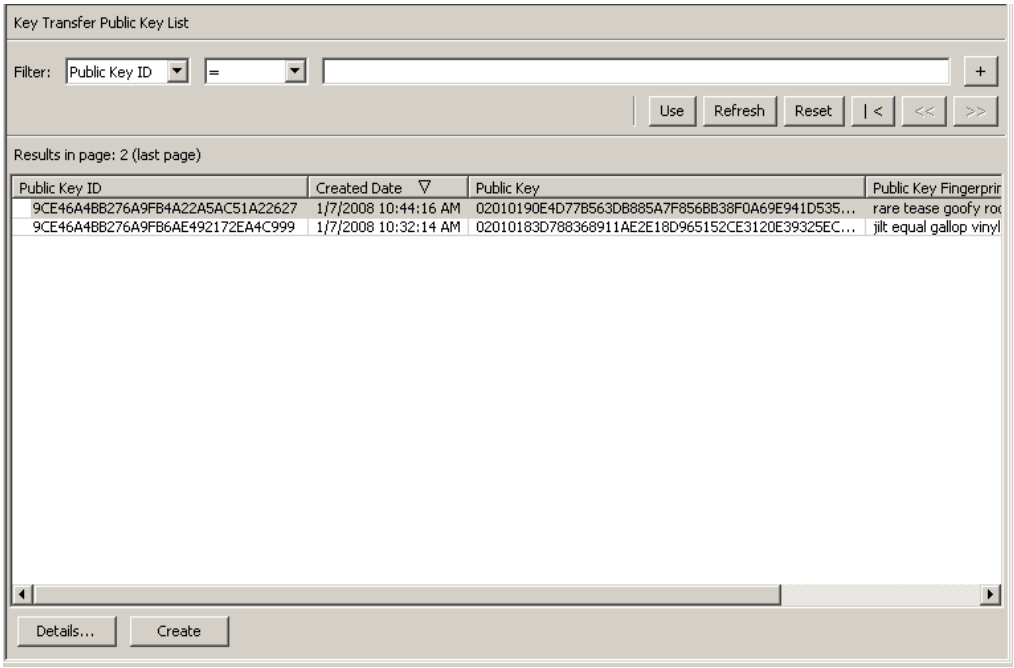
転送パートナー間で鍵を共有する場合、セキュリティー責任者は、まず自身の OKM クラスタの公開鍵情報にアクセスする必要があります。このメニューを使用すると、公開鍵情報を表示できます。このコマンドで表示される公開鍵と公開鍵 ID を、転送パートナーに送信する必要があります。



「Key Transfer Public Key List」の表示

鍵転送用の公開鍵リストを表示するには、次の手順を実行します。

1. 「System Management」メニューから、「**Key Transfer Public Key List**」を選択します。



データベース全体をスクロールするか、次のいずれかのキーで鍵転送用公開鍵リストにフィルタを適用することもできます。

- Public Key ID
- 作成日
- Public Key

表示されている鍵転送用公開鍵リストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ：

表示されている公開鍵のリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタの条件を満たす公開鍵のみが表示されます。

フィルタ属性コンボボックス：

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。取り得る値は次のとおりです。

- Public Key ID
- 作成日
- Public Key

フィルタ演算子コンボボックス :

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス :

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用 :

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Public Key ID:

各公開鍵を識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。この属性でソートするには、この列名をクリックします。

作成日 :

この公開鍵が作成された日時が表示されます。この属性でソートするには、この列名をクリックします。

もっとも最近作成された公開鍵に対応する非公開鍵は、エクスポートされたすべての鍵転送ファイルの署名に使用されます。

公開鍵

転送パートナー間での鍵転送の実行に使用される公開鍵が表示されます。この値は、Base 64 で表示されます。この属性でソートするには、この列名をクリックします。

Public Key Fingerprint:

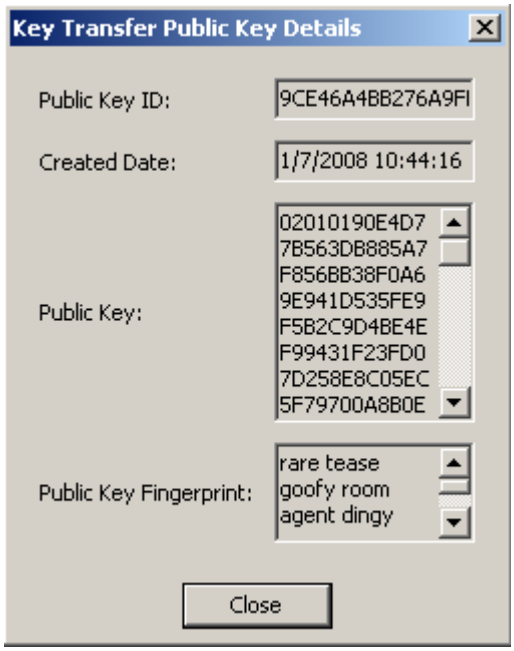
公開鍵のハッシュ値が表示されます。これは公開鍵が正しく転送されたことを確認するために使用する値で、Base 64 で表示されます。

鍵転送用公開鍵の詳細の表示

「Key Transfer Public Key Details」画面を表示するには、次の手順を実行します。

1. 公開鍵を選択して「**Details**」ボタンをクリックします。

   「Key Transfer Public Key Details」ダイアログボックスが表示されます。

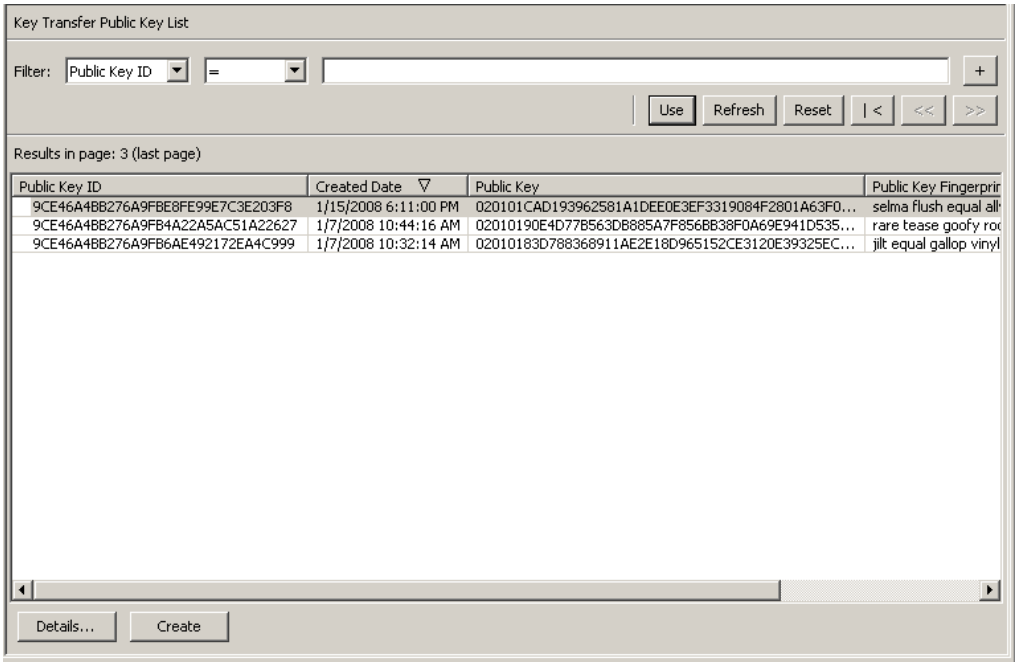


鍵転送用公開鍵の作成

鍵転送用公開鍵を作成するには、次の手順を実行します。

1. 「**Create**」ボタンをクリックします。
2. 新しい鍵を既存のすべての転送パートナーに提供します。

   新しい鍵転送用公開鍵の作成後に作成したすべての鍵転送ファイルは、新しい鍵転送用公開鍵で署名されるため、パートナーに新しい鍵転送用公開鍵を提供しないと、パートナーは新しい鍵転送ファイルをインポートできません。



「Backup List」メニュー

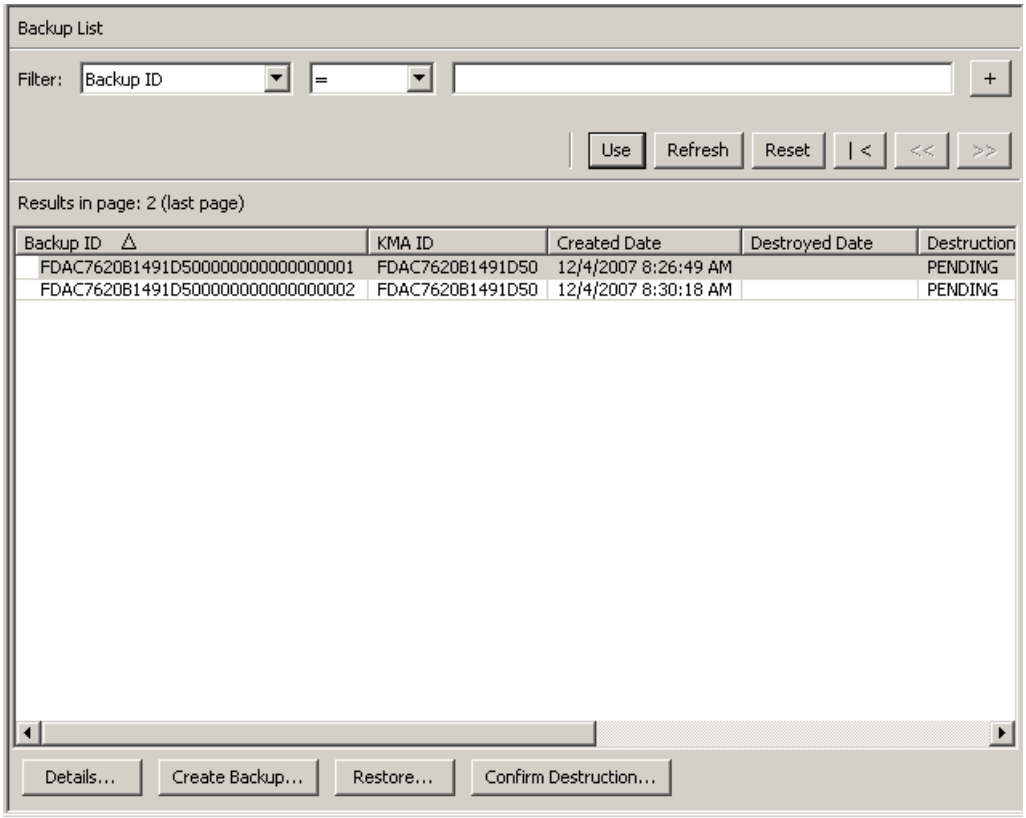
「Backup List」メニューオプションを使用すると、セキュリティー責任者は、次の操作を行うことができます。

- バックアップの履歴の表示
- バックアップファイルの詳細の表示
- バックアップの復元

バックアップファイルの履歴の表示

バックアップファイルの履歴を表示するには、次の手順を実行します。

「Secure Information Management」メニューから、「**Backup List**」を選択します。「Backup List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでバックアップファイルにフィルタを適用することもできます。

- Backup ID
- KMA ID
- 作成日
- Destroyed Date
- Destruction Status
- Destruction Comment

表示されているバックアップファイルのリストにフィルタを適用するには、「+」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- Backup ID
- 作成日
- Destroyed Date
- Destruction Status
- Destruction Comment

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~

フィルタ値 1 ボックス :

日付フィルタを選択した場合は、「**Set Date**」をクリックして開始日時を指定します。値は、フィルタキーの範囲の開始値として表示されます。ほかのフィルタを選択した場合は、このフィールドに値を入力します。

フィルタ値 2 ボックス :

日付フィルタを選択した場合は、「**Set Date**」をクリックして終了日時を選択します。値は、フィルタキーの範囲の終了値として表示されます。

使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

バックアップファイルが生成された KMA が表示されます。

作成日

バックアップが作成された日時が表示されます。

Destroyed Date

バックアップファイルが手動で破棄とマークされた日時が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。取り得る値は次のとおりです。

NONE

バックアップファイルは破棄されておらず、ファイルには破棄されたデータユニットの鍵は含まれていません。

PENDING

バックアップファイルはまだ手動で破棄されておらず、ファイルには破棄されたデータユニットの鍵のコピーが含まれています。

DESTROYED

バックアップファイルは手動で破棄されています。

Destruction Comment

バックアップファイルの破棄に関するユーザーが指定した情報が表示されます。

詳細 :

このボタンをクリックすると、バックアップの詳細情報が表示されます。

Create Backup:

このボタンをクリックすると、バックアップが作成されます。セキュリティー責任者の場合、このボタンは使用不可になっています。

復元 :

このボタンをクリックすると、バックアップが復元されます。

Confirm Destruction:

このボタンをクリックすると、バックアップの破棄を確認できます。セキュリティー責任者の場合、このボタンは使用不可になっています。

バックアップの詳細情報を表示する場合は、そのバックアップを強調表示して「**Details**」ボタンをクリックします。詳細については、199 ページの「バックアップの詳細の表示」を参照してください。

現在選択しているバックアップを復元するには、「**Restore**」ボタンをクリックします。詳細については、201 ページの「バックアップの復元」を参照してください。

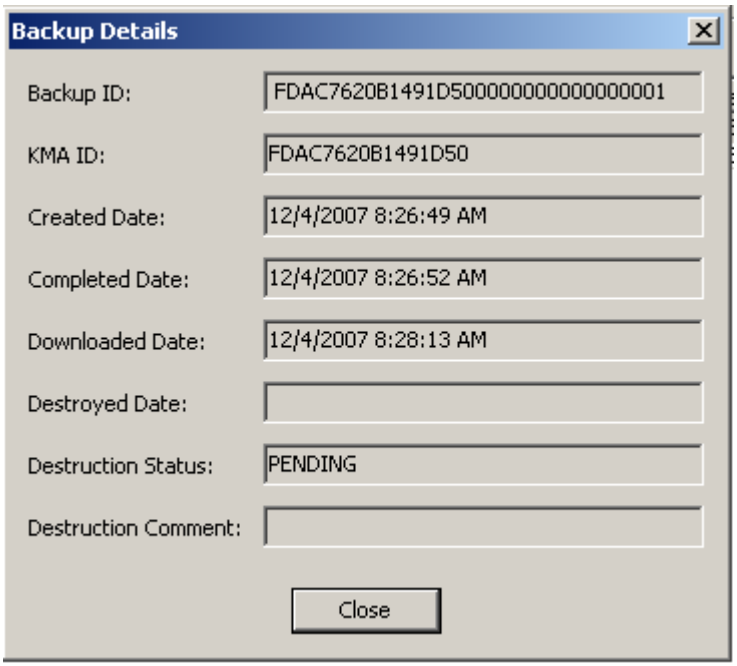
バックアップの詳細の表示

「Backup Details」ダイアログボックスは、バックアップファイルの詳細を表示する場合に使用します。

> **注 ー** バックアップファイルは KMA 上で作成および復元されます。

バックアップファイルの詳細を表示するには、次の手順を実行します。

1. 「Backups List」画面で、詳細情報を表示するバックアップエントリをダブルクリックするか、またはバックアップエントリを強調表示して「**Details**」ボタンをクリックします。「Backup Details」ダイアログボックスが表示され、すべてのフィールドが読み取り専用になっています。



2. 次に、フィールドとその説明を示します。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

このバックアップファイルが生成された KMA が表示されます。

作成日

バックアップファイルが作成された日時が表示されます。

Completed Date

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date

バックアップファイルがダウンロードされた日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日付が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。

Destruction Comment

バックアップファイルの破棄に関するユーザーが指定した情報が表示されます。

3. このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。

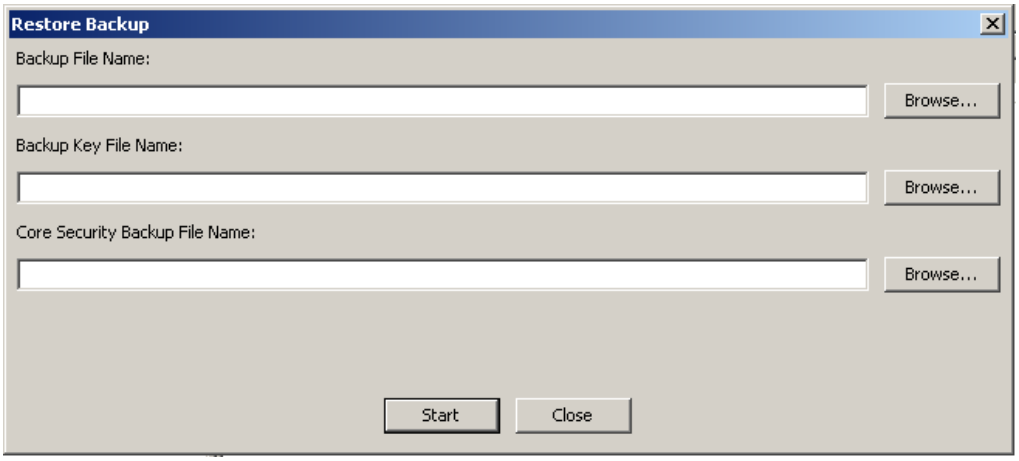
バックアップの復元

この機能を使用すると、バックアップファイルとバックアップ鍵ファイルで構成されるバックアップをアップロードして KMA に復元できます。バックアップファイルを KMA に復元する前に、認証に必要な定足数を満たしているかどうかを確認してください。

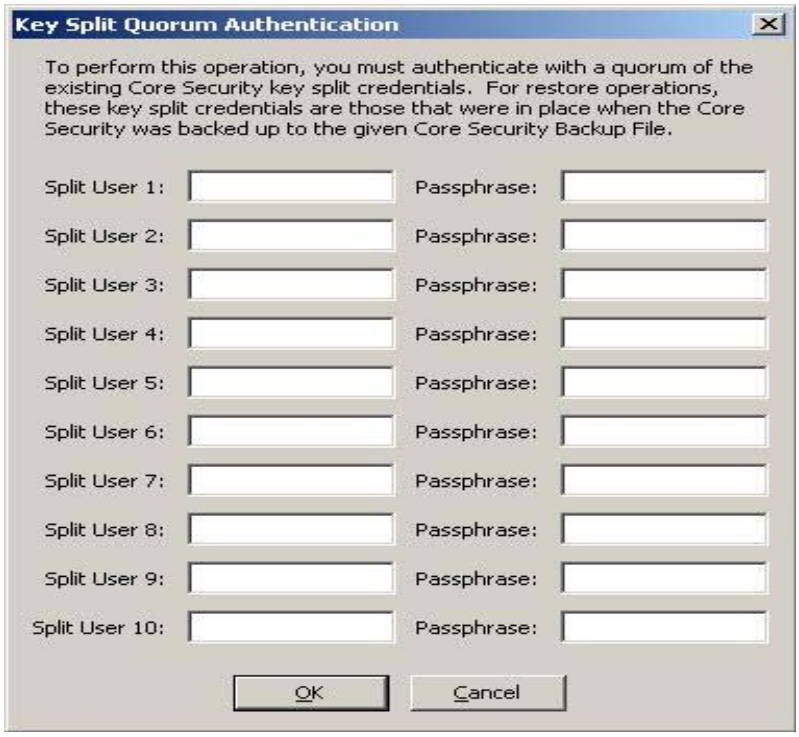
重要 – この手順を開始する前に、71 ページの「クラスタのバックアップからの復元」の手順を実行する必要があります。

バックアップを復元するには、次の手順を実行します。

1. 「Backup List」画面で、復元するバックアップを強調表示して「**Restore**」ボタンをクリックします。「Restore Backup」ダイアログボックスが表示されます。
2. 必要なコアセキュリティーバックアップ、バックアップ鍵ファイル、およびバックアップファイルを選択します。バックアップ鍵ファイルとバックアップは、一致している必要があります。つまり、同時に作成されている必要があります。コアセキュリティーバックアップは、バックアップ鍵ファイルとバックアップファイルより古い場合または新しい場合があります。コアセキュリティーバックアップファイルは、任意のバックアップ鍵ファイルおよびバックアップファイルとともに使用できます。
3. 「**Start**」ボタンをクリックします。



4. アップロード処理が完了すると、「Restore Backup」ダイアログボックスに完了したことが示され、「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



注 ー セキュリティー責任者は、鍵分割資格の十分な定足数を指定する必要があります。「Key Split Threshold」の値を最初に設定します。これにより、58 ページの「鍵分割資格の入力」の操作を通して、定足数のサイズが決定されます。定足数の値は、216 ページの「鍵分割設定の変更」で説明する手順を使用して変更できます。

「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

5. 「Restore Backup」ダイアログボックスが表示され、復元処理の状態が示されます。

6. 次に、フィールドとその説明を示します。

Backup File Name

バックアップファイルの名前です。

Backup Wrapping Key File Name

バックアップ鍵ファイルの名前が表示されます。

Core Security Backup File Name

コアセキュリティー鍵データを含むバックアップファイルの名前です。

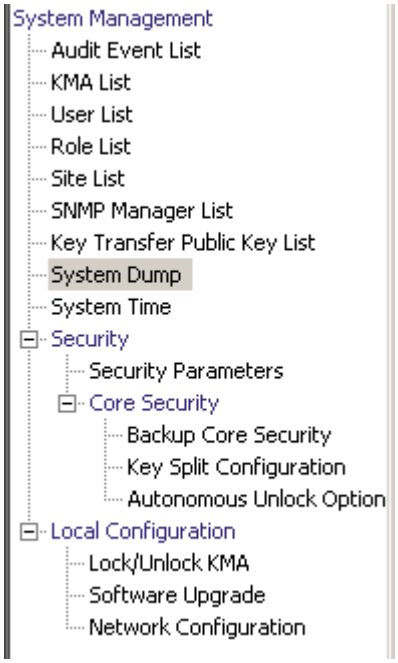
7. 復元が完了すると、完了を示すメッセージが表示されます。このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。データベースとセキュリティー保護された鍵ストアが、KMA に復元されます。

> **注 ー** バックアップを正常に復元したあとに、KMA の IP アドレス設定を更新する必要があります。ネットワーク設定はバックアップされないため、復元されません。364 ページの「KMA の管理 IP アドレスの設定」および 366 ページの「KMA のサービス IP アドレスの設定」を参照してください。

「System Dump」メニュー

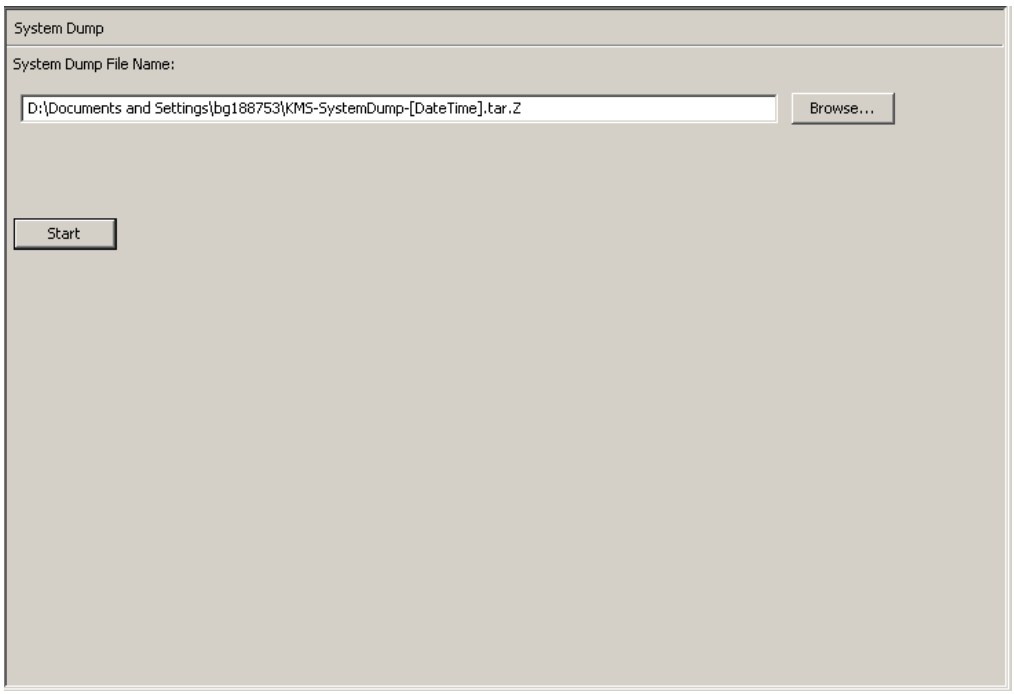
「System Dump」メニューでは、問題解決のためのシステムダンプを作成し、OKM Manager が動作しているシステム上の圧縮ファイルにダウンロードします。ダウンロードしたファイルは、圧縮ユーティリティーで開くことができる形式になっています。

注 – ダンプには、鍵データまたは鍵を推測するために使用できる情報は含まれていません。



システムダンプの作成

1. システムダンプを作成するには、「System Management」メニューから、「**System Dump**」を選択します。画面が表示され、自動生成された *.tar.Z ファイルが表示されます。必要に応じて、「Browse」をクリックして出力先のパスを選択できます。
2. 「**Start**」ボタンをクリックしてダウンロードを開始します。ダウンロードされたシステムダンプ情報のサイズをリアルタイムで示すメッセージが表示され、処理の完了が通知されます。
3. 出力先のパスに移動し、*.tar.Z ファイルを開いてシステムダンプ情報を表示します。



次に、フィールドとその説明を示します。

ファイル名 :

自動生成された *.tar.gz ファイルが表示されます。

参照 :

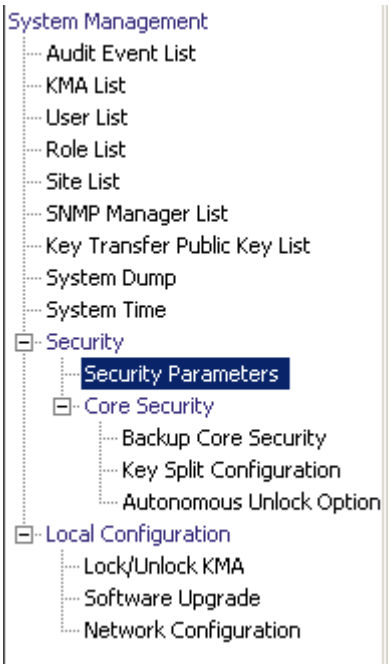
このボタンをクリックすると、このファイルの場所を指定できます。

開始 :

このボタンをクリックすると、ダウンロード処理が開始されます。

「Security Parameters」メニュー

「Security」メニューを使用すると、セキュリティー責任者は、KMA のセキュリティーパラメータを表示および変更できます。



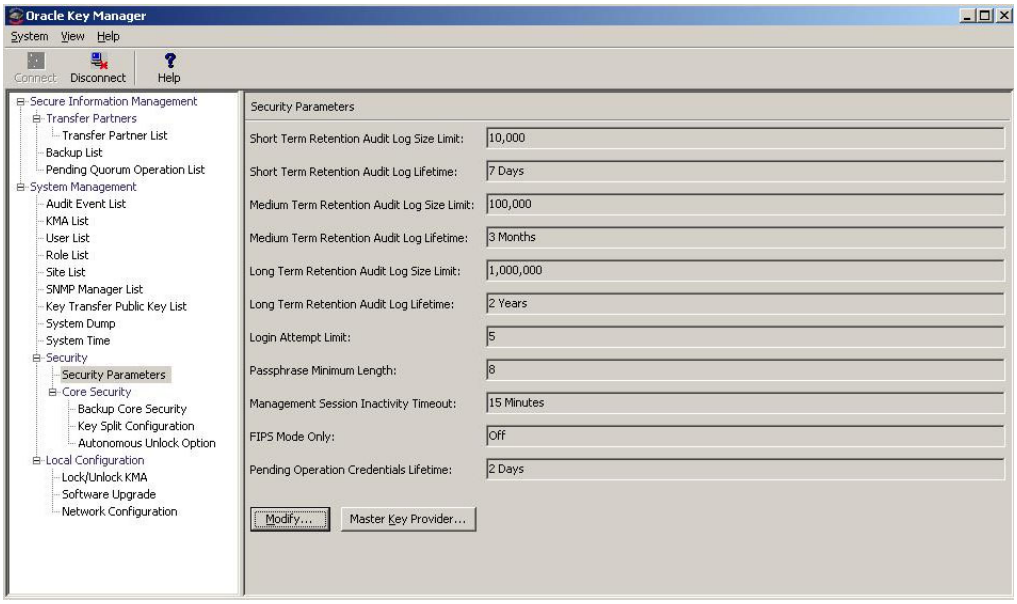
セキュリティーパラメータの取り出し

注 ー 「**Master Key Provider**」ボタンは、OKM クラスタで IBM メインフレームからマスター鍵を取得する場合にのみ使用します。このボタンは、OKM クラスタの複製バージョンが現在 11 以降に設定されており、「FIPS Mode Only」の値が「Off」の場合にのみ使用可能です。

詳細は、『OKM-ICSF Integration Guide』を参照してください。

セキュリティーパラメータを取り出すには、次の手順を実行します。

「Security」メニューから、「**Security Parameters**」を選択します。「Security Parameters」画面が読み取り専用モードで表示されます。



次に、フィールドとその説明を示します。

注 ー 次の 6 つの保持関連フィールドについては、1 つの監査ログのみが存在し、そのログは KMA 内の最大のファイルシステムに格納されます。

これらのパラメータを調整する主な目的は、「Audit Event List」メニューから実行するクエリーで返される監査ログエントリの数を制御することです (282 ページの「監査ログの表示」を参照)。

監査ログのエントリは、短期、中期、または長期の保持期間を示すことができます。KMA は、エントリの保持期間の制限および有効期間に基づいて、古い監査ログエントリを切り捨てます (削除します)。

たとえば、短期監査ログエントリは通常、中期監査ログエントリよりも頻繁に切り捨てられ、中期監査ログエントリは長期監査ログエントリよりも頻繁に切り捨てられます。

セキュリティー責任者は、これらの保持期間の制限および有効期間を定義することによって、古い監査ログエントリが削除される頻度を制御できます。

Short Term Retention Audit Log Size Limit

短期監査ログエントリの保持数が表示されます。この数を過ぎるとエントリは切り捨てられます。デフォルトは 10,000 分です。最小値は 1000、最大値は 1,000,000 です。

Short Term Retention Audit Log Lifetime

短期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、7 日です。最小値は 7 日、最大値は 25,185 日 (約 69 年) です。

Medium Term Retention Audit Log Size Limit

中期監査ログエントリの保持数が表示されます。この数を過ぎるとエントリは切り捨てられます。デフォルト値は 100,000 です。最小値は 1000、最大値は 1,000,000 です。

Medium Term Retention Audit Log Lifetime

中期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、90 日です。最小値は 7 日、最大値は 25,185 日です。

Long Term Retention Audit Log Size Limit

長期監査ログエントリの保持数が表示されます。この数を過ぎるとエントリは切り捨てられます。デフォルト値は 1,000,000 です。最小値は 1000、最大値は 1,000,000 です。

Long Term Retention Audit Log Lifetime

長期監査ログエントリの保持期間 (日数) が表示されます。この期間を過ぎるとエントリは切り捨てられます。デフォルトは、730 日です。最小値は 7 日、最大値は 25,185 日です。

Login Attempt Limit

失敗が許容されるログイン試行の回数が示されます。この回数を過ぎると実体は使用不可になります。デフォルトは 5 分です。最小値は 1、最大値は 1000 です。

Passphrase Minimum Length

パスフレーズの最小文字数が表示されます。デフォルトは、8 文字です。最小文字数は 8 文字、最大文字数は 64 文字です。

Management Session Inactivity Timeout

OKM Manager またはコンソールのログインセッションをアイドルにしておくことができる最長時間 (分単位) が表示されます。この時間を過ぎると、ログインセッションは自動的にログアウトされます。この値を変更しても、すでに進行中のセッションには影響を及ぼしません。デフォルトは、15 分です。最小値は 0 分 (アイドル時間なし)、最大値は 60 分です。

FIPS Mode Only

鍵および形式転送ファイルのインポートの設定が表示されます。

値「Off」は、AES 鍵ラップをサポートするエージェントと通信するときは常に KMA が鍵をラップするように指定します。ほとんどの顧客は、AES 鍵ラップをサポートするテープドライブファームウェアを OKM エージェントサービスで実行しているはずです。

OKM をサポートするすべての PKCS#11 プロバイダには、AES 鍵ラップのサポートが含まれています。これは、OKM 監査ログを表示して、エージェントが次に示すエージェントサービスの操作を使用していることを確認することによって、確認できます。「Operation」に対して監査フィルタを指定し、プルダウンリストから次の特定の操作を選択します。

- Create Key v2
- Retrieve key v2
- Retrieve Keys v2
- Retrieve Protect and Process Key v2

結果リストに監査イベントがある場合、指定したエージェントは OKM で AES 鍵ラップを使用しています。

値「On」は、このクラスタ内の KMA が、鍵をエージェント (テープドライブ) に送信する前に、Advanced Encryption Standard (AES) ラッピング鍵で鍵をラップすることを指定します。KMA では、1.0 の鍵をインポートできず、v2.1 (FIPS) の形式転送ファイルに限りエクスポートおよびインポートが可能です。

値「On」は、現在の複製バージョンが 10 以降の場合にのみ設定できます。

詳細は、175 ページの「「Transfer Partner List」メニュー」の「Export Format」パラメータを参照してください。

Pending Operation Credentials Lifetime:

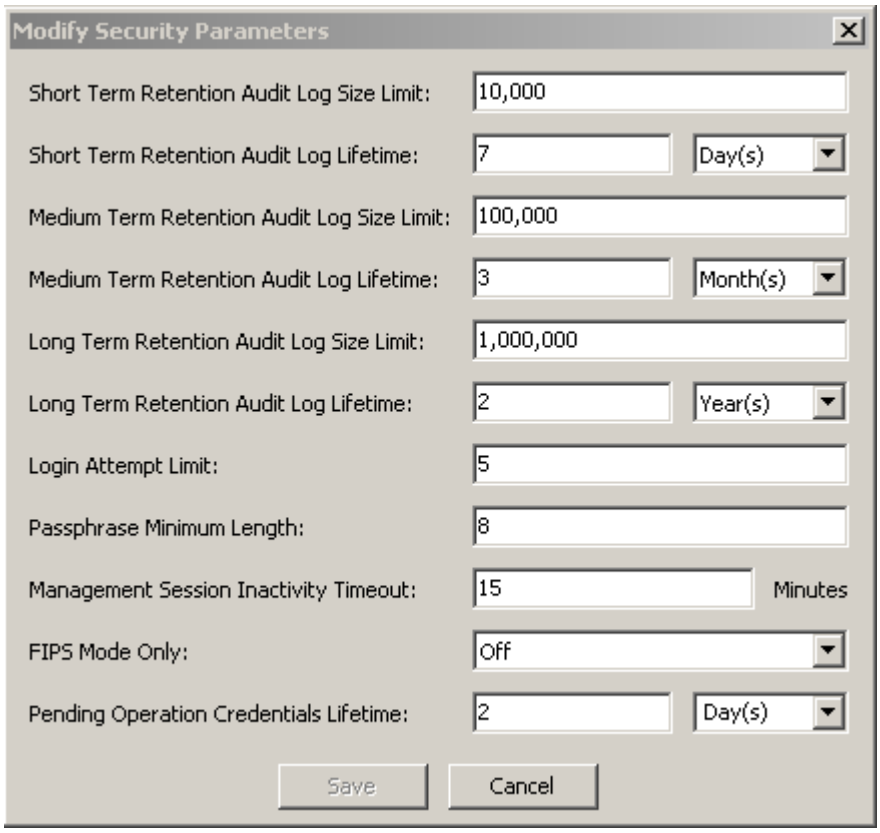
保留中の定足数操作を承認したものとして鍵分割資格が保持される期間 (日数) です。保留中の定足数操作をこの有効期間内に承認する鍵分割資格の数が不足している場合、これらの資格は期限切れになります。期限切れになったあとは、定足数メンバーが、保留中の定足数操作を再承認する必要があります。デフォルトは、2 日です。この値は、複製バージョンが 11 以降の場合にのみ使用されます。

セキュリティーパラメータを変更する場合は、「Modify」ボタンをクリックします。詳細については、211 ページの「セキュリティーパラメータの変更」を参照してください。

セキュリティーパラメータの変更

セキュリティーパラメータを変更するには、次の手順を実行します。

1. 「Security Parameters List」画面で、「**Modify**」ボタンをクリックします。「Modify Security Parameters」画面が表示されます。



フィールドについては 208 ページで説明します。

2. 必要に応じて、セキュリティーパラメータを変更します。終了したら、「**Save**」ボタンをクリックします。変更内容が KMA データベースに保存されます。

コアセキュリティー

コアセキュリティーコンポーネントの主な要素は、ルート鍵データです。ルート鍵データとは、クラスタの初期化時に生成される鍵データです。ルート鍵データによって、マスター鍵が保護されます。マスター鍵とは、KMA に格納されるデータユニット鍵を保護する対称鍵です。

コアセキュリティーは、鍵分割スキーマによって保護されます。このスキーマでは、ルート鍵データのラップを解除するために、鍵分割資格で定義された定足数のユーザーのユーザー名とパスフレーズを提供する必要があります。

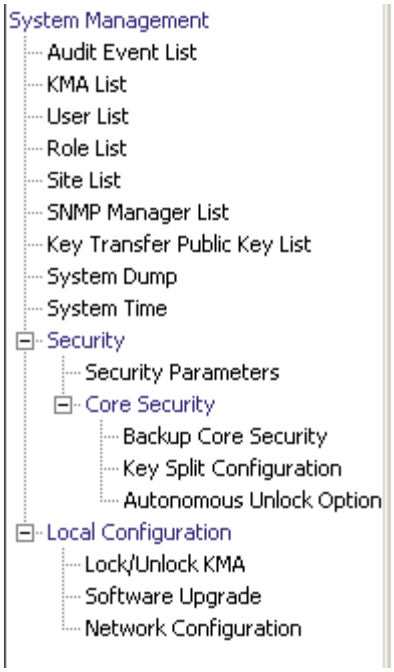
このセキュリティーメカニズムでは、KMA に対して*ロック*と*ロック解除*の 2 つの操作状態が有効になります。

*ロック状態*の KMA では、ルート鍵データのラップを解除できないため、データユニット鍵にアクセスできません。このため、KMA では、新しいデータユニットを登録するか、または既存のデータユニットのデータユニット鍵を取り出すエージェントの要求を処理できません。

*ロック解除*状態の KMA では、ルート鍵データを使用してデータユニット鍵にアクセスし、エージェントのデータユニット鍵の要求を処理できます。

「Core Security」メニュー

「Core Security」メニューには、次のメニューオプションがあります。



このメニューを使用すると、セキュリティー責任者は、次の操作を行うことができます。

- コアセキュリティーバックアップの作成
- 鍵分割資格の表示および変更
- 自律ロック解除オプションの使用可能および使用不可への切り替え

Backup Core Security

「Backup Core Security」オプションを使用すると、セキュリティー責任者は、コアセキュリティー鍵データをバックアップしてローカルシステムのファイルにダウンロードできます。

> **注意 ー** コアセキュリティーバックアップファイルは、注意して保護してください。コアセキュリティーバックアップファイルは、任意のバックアップファイルとバックアップ鍵ファイルのペアとともに使用できるため、以前のコアセキュリティーバックアップファイルでも使用できます。

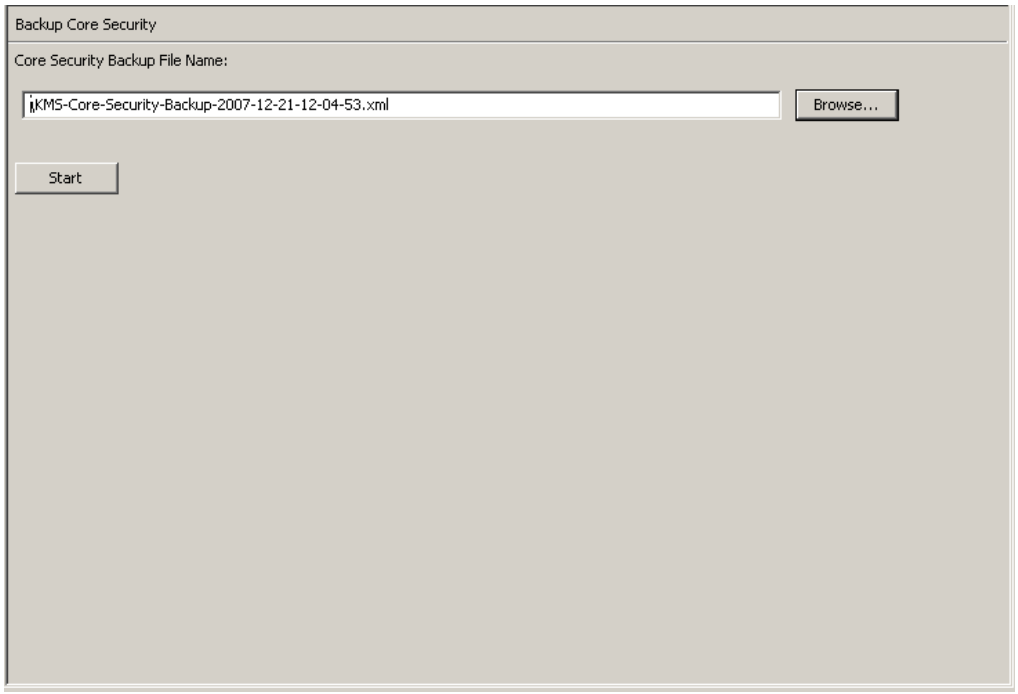
コアセキュリティーバックアップの作成

鍵分割資格の変更後は、新しいコアセキュリティーバックアップの実行が必要になります。

重要 – セキュリティー責任者がコアセキュリティー鍵データをバックアップしたあとでないと、バックアップ担当者はバックアップを作成できません。329 ページの「バックアップの作成」を参照してください。

1. 「Core Security」メニューから、「Backup Core Security」を選択します。「Backup Core Security」ダイアログボックスが表示されます。

   > **注 ー** コアセキュリティーバックアップファイルの名前は、自動的に生成されます。ただし、名前を編集するか、「Browse」ボタンをクリックして出力先のパスを選択することもできます。



2. 「**Start**」ボタンをクリックしてコアセキュリティーバックアップファイルを作成し、ユーザー指定の出力先にダウンロードします。

3. バックアップが完了すると、メッセージが表示されます。このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。
4. 「Backup Core Security」画面に戻ります。

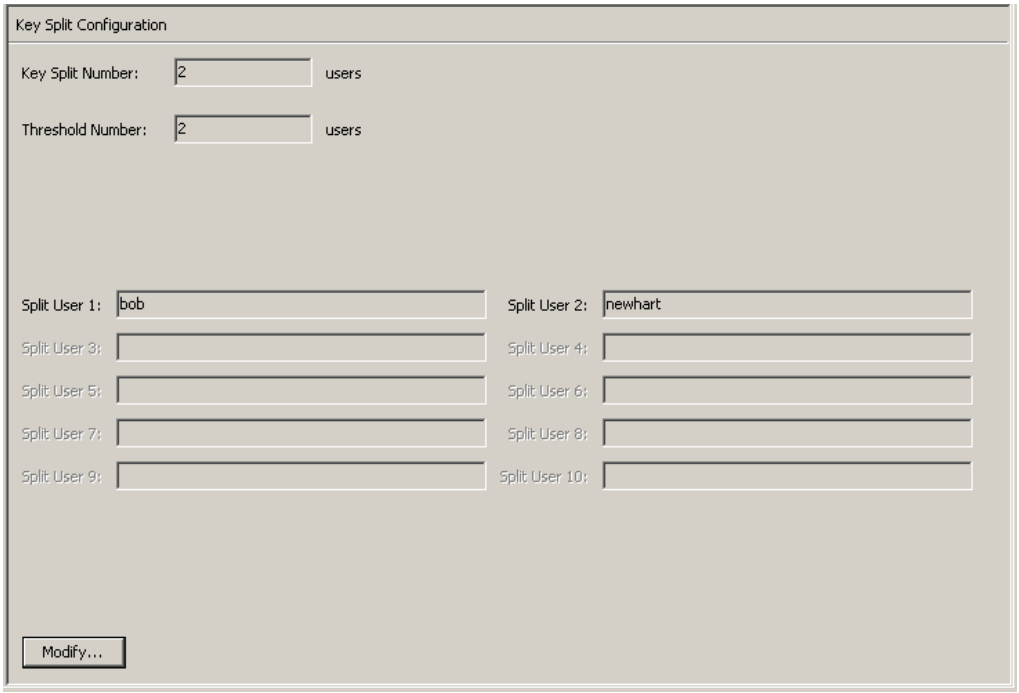
Key Split Configuration

「Key Split Configuration」メニューオプションを使用すると、セキュリティー責任者は、KMA の鍵分割資格を表示および変更できます。

鍵分割設定の表示

鍵分割設定を表示するには、次の手順を実行します。

1. 「Core Security」メニューから、「**Key Split Configuration**」をクリックします。「Key Split Configuration」ダイアログボックスが表示されます。



次に、フィールドとその説明を示します。

Key Split Number

鍵の分割数が表示されます。最大数は 10 です。

Threshold Number

定足数の認証に必要なユーザー数が表示されます。

Split User (1 ～ 10)

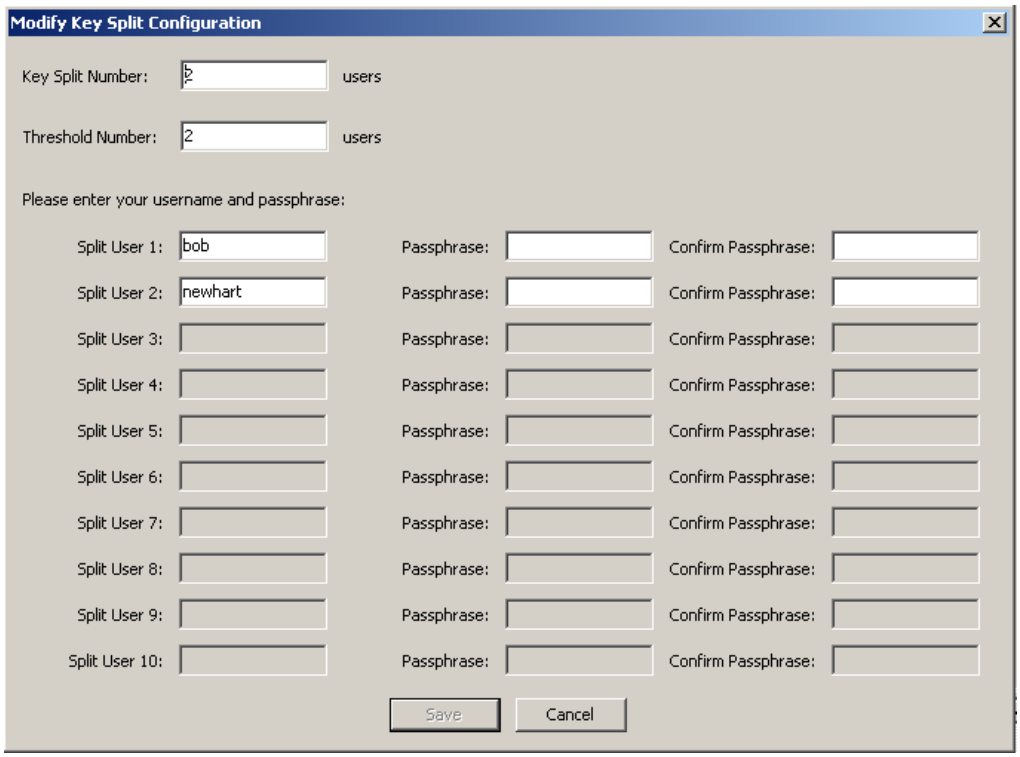
既存の分割のユーザー名が表示されます。

鍵分割のユーザー名、パスフレーズ、およびしきい値の数を変更する場合は、「**Modify**」ボタンをクリックします。詳細については、216 ページの「鍵分割設定の変更」を参照してください。

鍵分割設定の変更

鍵分割設定を変更するには、次の手順を実行します。

1. 「Key Split Configuration」画面で、「**Modify**」ボタンをクリックします。「Modify Key Split Configuration」ダイアログボックスが表示されます。



2. 次のパラメータを設定し、「**OK**」ボタンをクリックします。

Key Split Number

鍵分割数の新しい値を入力します。最大数は 10 です。

Threshold Number

定足数を満たすために必要なユーザー数の新しい値を入力します。

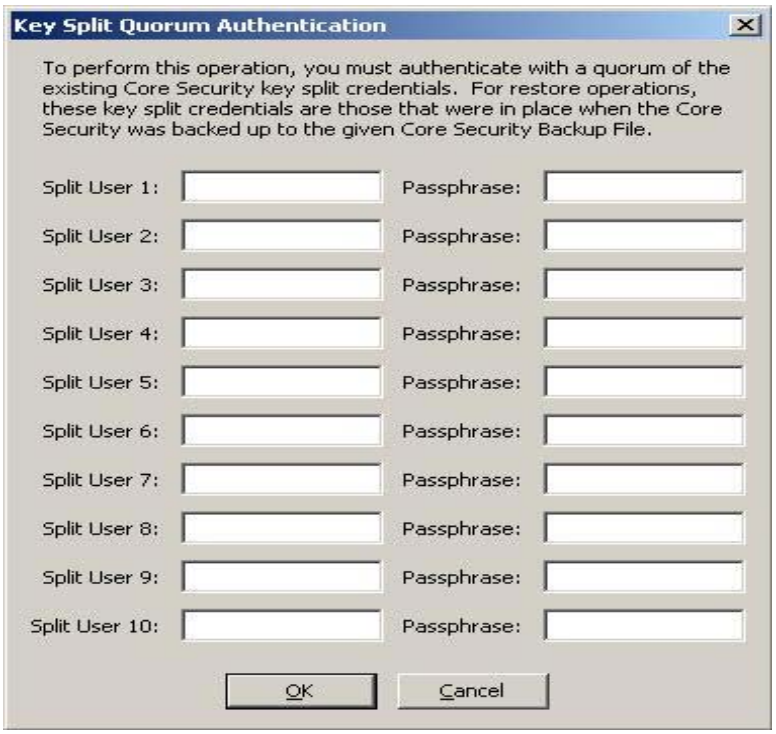
Split User *x*

ユーザー名を入力します。分割ユーザーごとに、関連する「Passphrase」フィールドと「Confirm Passphrase」に値を入力します。

> **注 ー** 入力できる分割ユーザーのフィールド数は、「Key Split Number」フィールドに入力した値によって決定されます。

3. 最後のユーザー名とパスフレーズを入力したあと、「**Save**」ボタンをクリックします。

4. 新しい鍵分割資格が入力されると、「Key Split Quorum Authentication」ダイアログボックスが表示されます。既存の定足数資格のユーザー名とパスフレーズを入力し、「**OK**」ボタンをクリックします。手順 2 および手順 3 の「新しい」資格を設定するには、この操作が必要です。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**Save**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

5. データベースの以前の設定情報が新しい設定に更新されます。新しい設定が「Key Split Credentials」画面に表示されます。

   注 ー 更新された鍵分割資格を使用して、コアセキュリティー鍵データがラップし直されます。

6. 新しいコアセキュリティーバックアップを作成します (214 ページの「コアセキュリティーバックアップの作成」を参照)。

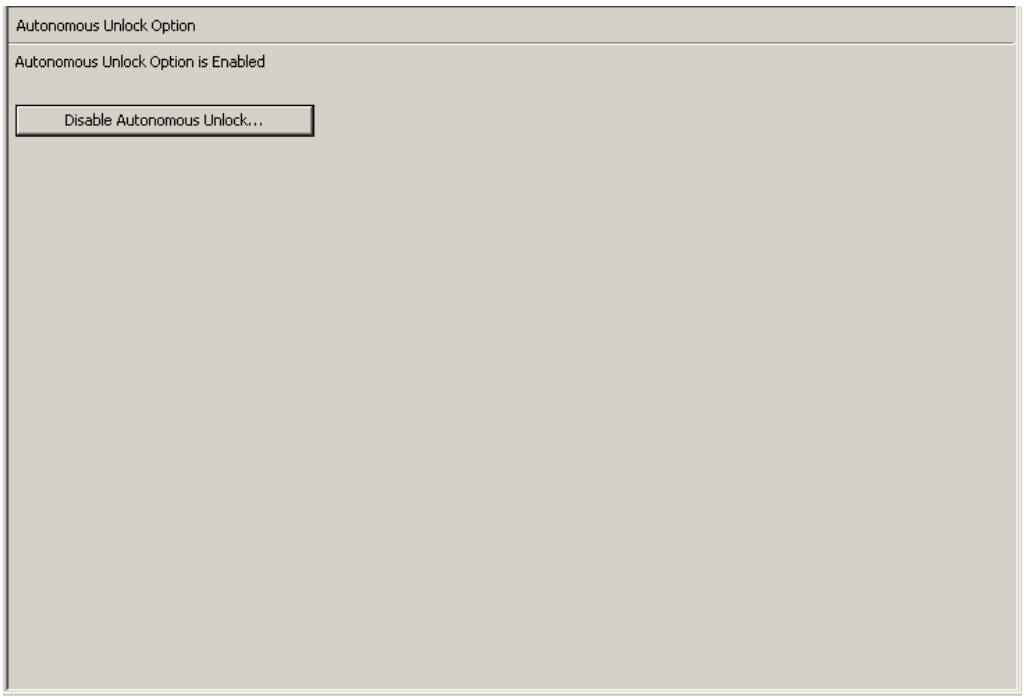
   注 ー 以前のコアセキュリティーバックアップファイルをすべて破棄して、以前の鍵分割資格がバックアップの破棄に使用できないようにする必要があります。

Autonomous Unlock Option

「Autonomous Unlock Option」メニューオプションを使用すると、セキュリティー責任者は、KMA の自律オプションを使用可能または使用不可に切り替えることができます。

自律ロック解除オプションを使用可能または使用不可に切り替えるには、次の手順を実行します。

1. 「Core Security」メニューから、「**Autonomous Unlock Option**」を選択します。「Autonomous Unlock Option」画面が表示され、現在の自律オプションの状態が示されます。



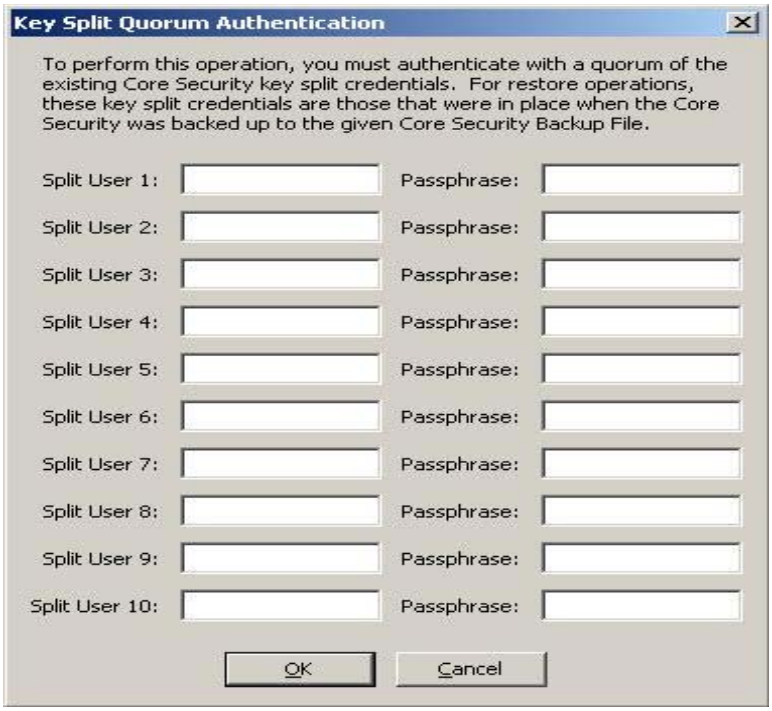
2. 現在の自律起動状態に従って、「**Enable Autonomous Unlock**」をクリックしてこのオプションを使用可能にするか、または「Disable Autonomous Unlock」をクリックしてオプションを使用不可にします。

   注 ー

   • 「**Lock/Unlock**」ボタンを使用すると、状態が切り替わり、KMA のロック状態が現在と反対の状態に設定されます。

   • 自律ロック解除オプションを使用可能または使用不可にするには、定足数を満たす必要があります。

3. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**Save**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

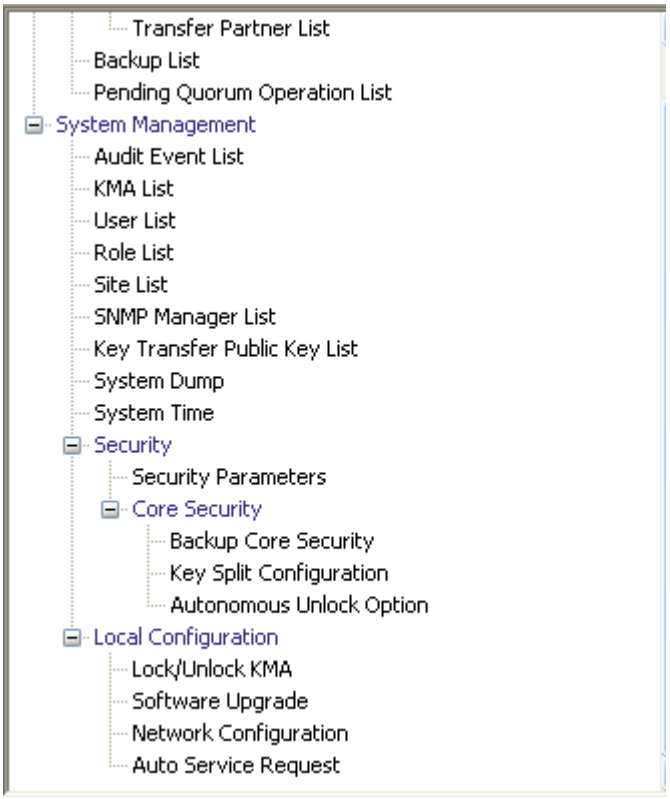
「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

「Local Configuration」メニュー

「Local Configuration」メニューには、次のオプションがあります。

- KMA のロックとロック解除
- ソフトウェアのアップグレード (321 ページの「「Software Upgrade」メニュー」を参照)
- ネットワーク構成情報
- Auto Service Request



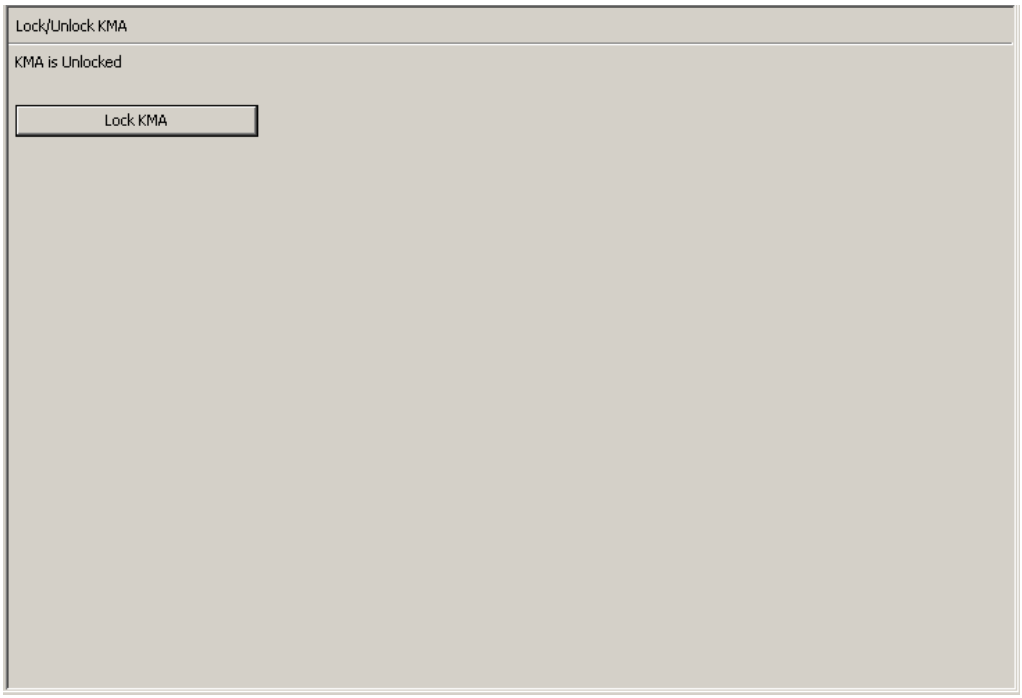
Lock/Unlock KMA

「Lock/Unlock KMA」メニューオプションを使用すると、セキュリティー責任者は、KMA のコアセキュリティーをロックまたはロック解除できます。コアセキュリティーと、コアセキュリティーがロックおよびロック解除されたときの KMA の動作の詳細は、212 ページの「コアセキュリティー」を参照してください。

KMA のロック

KMA をロックするには、次の手順を実行します。

1. 「Local Configuration」メニューから、「**Lock/Unlock KMA**」を選択します。「Lock/Unlock KMA」画面が表示され、KMA の状態が示されます。この例では、状態は「Unlocked」になっています。



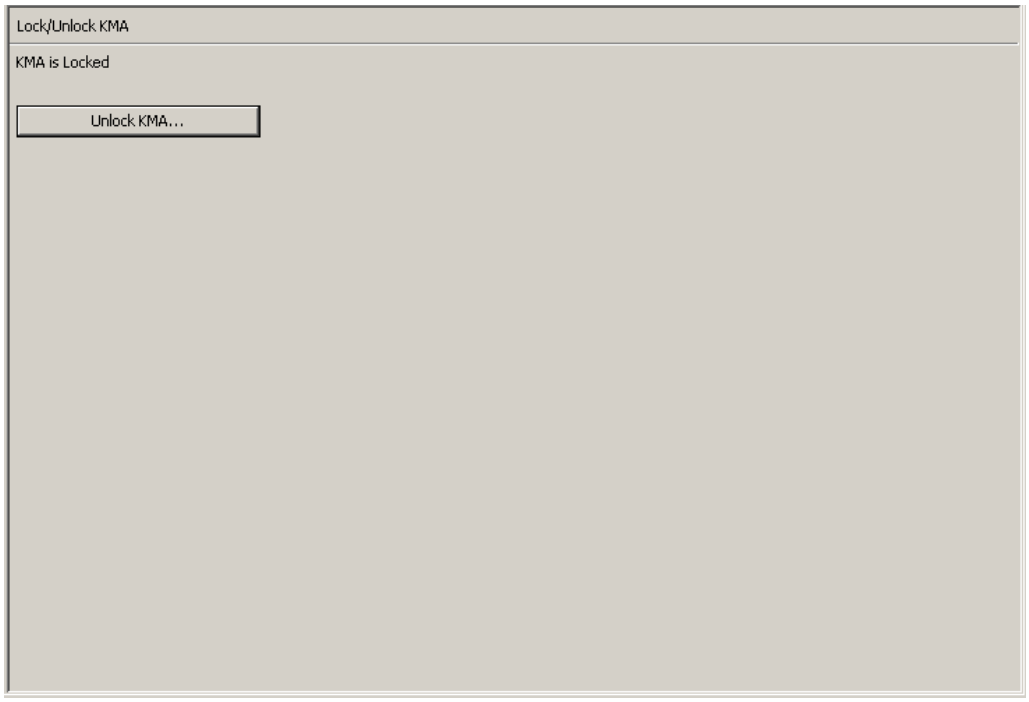
2. 「**Lock KMA**」ボタンをクリックして、KMA をロックします。ボタンを 1 回押すと、このボタンは「Unlock KMA」に変わり、新しいロック状態と実行できる操作が示されます。これで、KMA はロックされました。

> **注 ー** 「Lock **KMA**」ボタンと「**Unlock KMA**」ボタンを使用すると状態が切り替わり、KMA のロック状態が現在と反対の状態に設定されます。ボタンを 1 回押すと、テキストラベルとボタンラベルが変わり、新しいロック状態と実行できる操作が示されます。

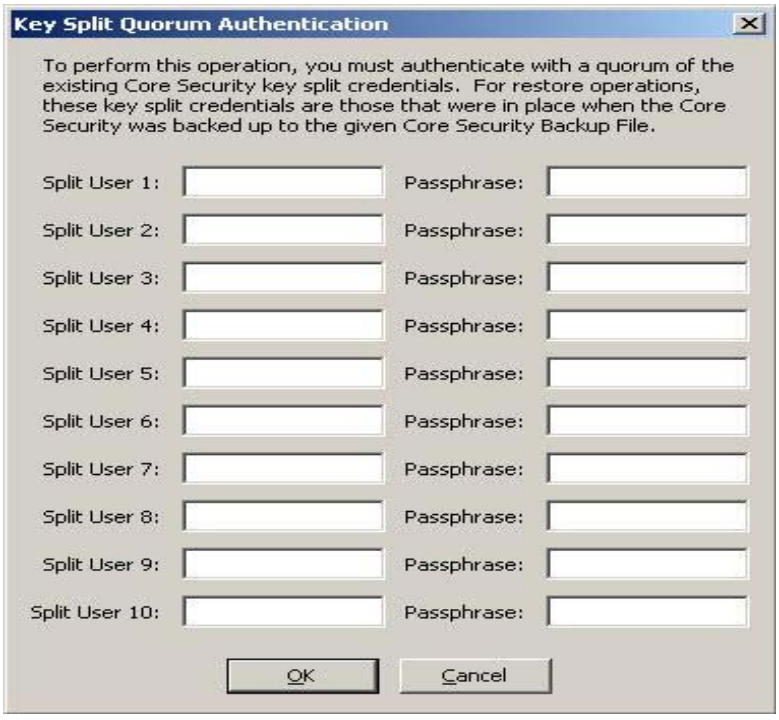
KMA のロック解除

KMA のロックを解除するには、次の手順を実行します。

1. 「Lock/Unlock KMA」画面で、「**Unlock KMA**」ボタンをクリックします。



2. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数分のユーザー名とパスフレーズを入力する必要があります。

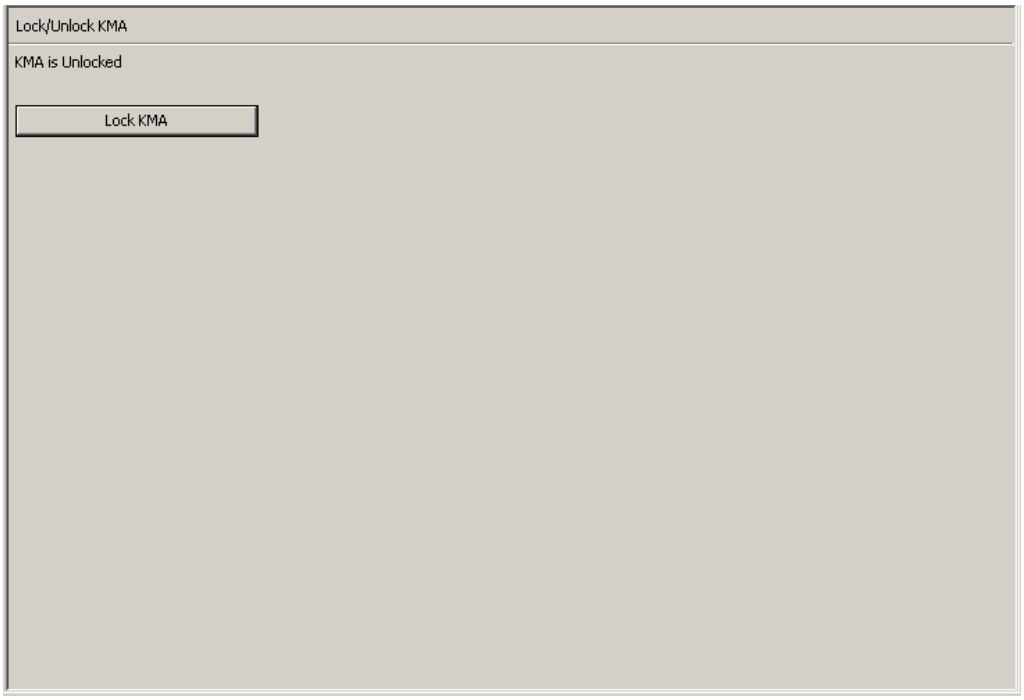


「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

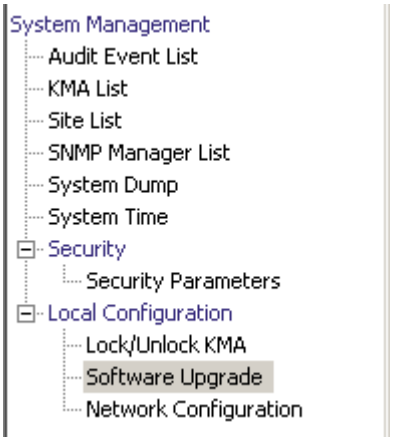
3. 認証が成功すると、「Key Split Quorum Authentication」ダイアログボックスが閉じ、KMA のロックが解除されます。


Lock/Unlock KMA
KMA is Unlocked
Lock KMA

ソフトウェアのアップグレード

「Software Upgrade」メニューオプションを使用すると、ソフトウェアアップグレードを適用できますが、これは 2 つの独立した手順で行う必要があります。

- オペレータはソフトウェアアップグレードファイルを KMA にアップロードし、アップグレードをただちに適用します。詳細は、322 ページの「ソフトウェアアップグレードのアップロードおよび適用」を参照してください。
- セキュリティー責任者は、オペレータがアップロードおよび適用した、アクティブでないソフトウェアバージョンをアクティブ化します。



ソフトウェア更新は Oracle によって署名され、適用前に KMA によって検証されます。

ソフトウェアアップグレードの実装のガイドライン

- この機能を実行する前に、システムをバックアップしてください。手順については、329 ページの「バックアップの作成」を参照してください。
- OKM Manager の GUI リリースは、KMA に読み込むアップグレードのバージョンと一致するものを使用してください。
- KMS 2.1 以前を実行している KMA を OKS 2.3 以降にアップグレードするには、まずその KMA を KMS 2.2 にアップグレードする必要があります。
- OKM Manager が KMA にリモート接続しているか、または OKM Manager と KMA の間の接続が低速な場合、アップロードと適用の処理に時間がかかる可能性があります。これを軽減するために、OKM Manager がインストールされているノートパソコンまたはワークステーション、および、KMA と同じサブネットに接続しているノートパソコンまたはワークステーションに、ソフトウェアアップグレードファイルをダウンロードできます。OKM Manager と KMA の間にルーターがある場合、アップグレード処理の速度が低下する場合があります。
- アップロードと適用の処理には、OKM Manager と KMA 間の接続環境が良好な場合でも、最短で約 30 分以上かかります。アクティブ化処理には、最短でも 5 - 15 分かかります。アップロード処理があまりに低速な場合、同じサブネットに KMA として接続してみてください。

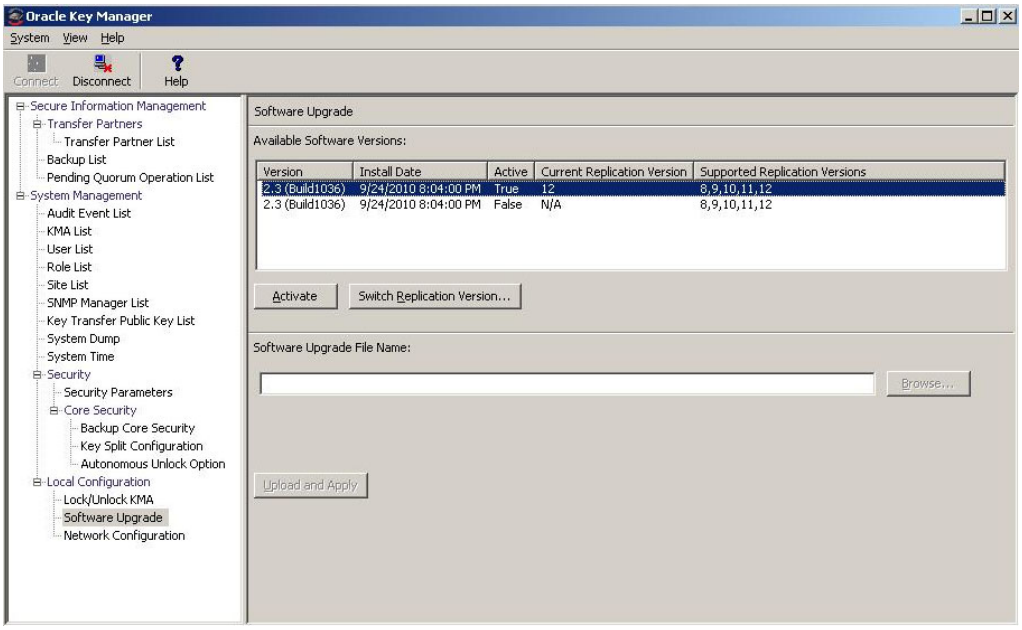
- (ネットワーク負荷の分散を促進するために) 各 KMA にソフトウェアアップグレードファイルを一度に 1 つずつアップロードおよび適用してから、(同時にオフラインになる KMA の数を最小化するために) 各 KMA で一度に 1 つずつソフトウェアアップグレードをアクティブ化してください。
- いずれかのアップグレード処理 (アップロード、検証、適用、アクティブ化、複製バージョンの切り替え) が失敗した場合、OKM Manager は、失敗の理由と提案する解決方法を説明する監査メッセージを生成します。
- アップグレードされた KMA では技術サポートアカウントが使用不可になっており、必要な場合はアカウントをふたたび使用可能にする必要があります。

ソフトウェアバージョンのアクティブ化

オペレータがソフトウェアアップグレードをアップロードおよび適用したあと、セキュリティー責任者は、オペレータがアップロードおよび適用したアクティブでないソフトウェアバージョンをアクティブ化する必要があります。

1. 「Local Configuration」メニューから、「**Software Upgrade**」を選択します。「Software Upgrade」画面が表示されます。

   ソフトウェアのアクティブなバージョンが強調表示され、「Active」列が「True」に設定され、アクティブでないバージョンが表示されます。



この画面には次のボタンが表示されます。

有効

アクティブでないソフトウェアバージョンを選択し、このボタンをクリックして、選択したソフトウェアバージョンをアクティブ化します。このソフトウェアバージョンがアクティブ化されることを知らせるメッセージが表示され、KMA が再起動します。

Switch Replication Version

アクティブなソフトウェアバージョンを選択し、このボタンをクリックして、現在の複製バージョンを切り替えます。

Software Upgrade File Name

オペレータがソフトウェアアップグレードファイルの名前を入力できます。

参照

オペレータはこのボタンをクリックして、ローカルシステム上のソフトウェアアップグレードファイルを指定できます。

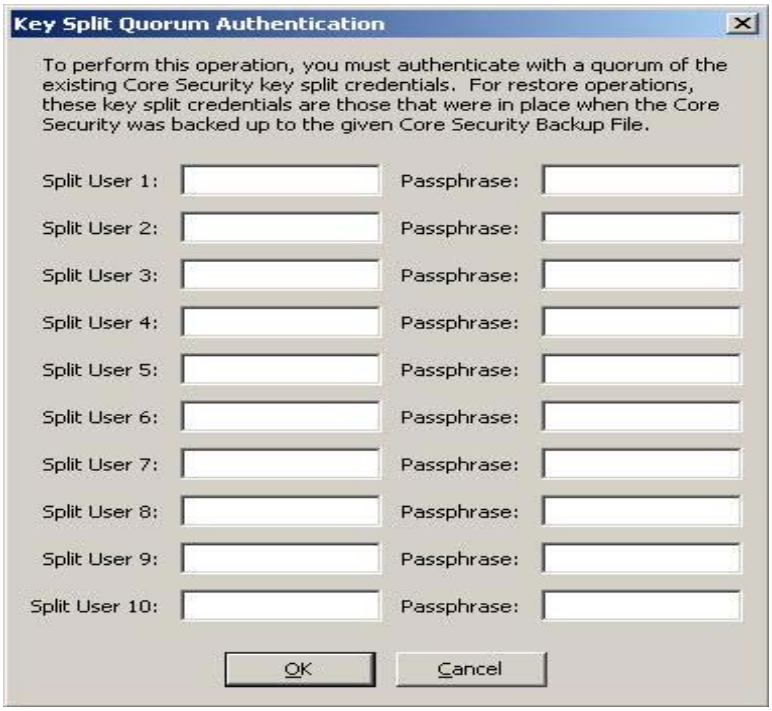
2. OKM クラスタの現在のバックアップが存在することを確認してください。

アップグレードファイルをアクティブ化するには、画面上部の使用可能バージョンのリストから新しいバージョンを選択して、「**Activate**」ボタンをクリックします。アクティブ化されるまで、新しいバージョンはシステム上でアクティブでない状態のままです。

> **注 ー** アクティブ化処理の途中で、KMA が再起動します。再起動の間は KMA がオフラインになるため、クラスタ内で複数の KMA を同時にアクティブ化することは望ましくない場合があります。

KMA を再起動するまで、ユーザーは接続されたままです。「Software Upgrade」画面にふたたびアクセスすると、新しくアップロードされたソフトウェアバージョンがアクティブなバージョンとして表示されます。

3. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。操作を認証するには、定足数の役割を持つユーザーのユーザー名とパスフレーズを入力する必要があります。



「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

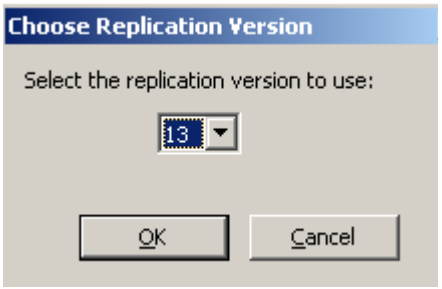
新しいソフトウェアバージョンには、OKM クラスタの複製バージョンをより大きな値に変更しないと使用可能にならない、新しい機能が含まれる場合があります。新しいソフトウェアバージョンの新しい機能をすべて使用可能にするには、OKM クラスタを新しい複製バージョンに切り替える必要があります。

複製バージョンの切り替え

最新のソフトウェアバージョンの一部の機能は、OKM クラスタの複製バージョンを、そのソフトウェアバージョンでサポートされている最大の値に設定しないと使用可能になりません。

複製バージョンはセキュリティー責任者が手動で設定します。自動的に変更されることはありません。

1. アクティブ化された KMA にログインし、「Software Upgrade」画面に移動します。「Supported Replication Versions」列の値が、「Current Replication Version」列よりも上位のバージョンである場合、「**Switch Replication Version**」ボタンをクリックします。



2. 新しい複製バージョンを選択して「**OK**」ボタンを選択します。

   「Current Replication Version」の表示が上位のバージョンに変わり、複製の正常な切り替えが、OKM クラスタ内のほかのすべての KMA に送信されます。

注 ー クラスタ内のすべての KMA が応答している必要があり、すべての KMA は、セキュリティー責任者が設定する複製バージョンをサポートする KMS または OKM のバージョンを実行している必要があります。

表 5-2 は、特定の複製バージョン (または、さらに上位のバージョン) を必要とする機能を、KMS および OKM のリリースごとにまとめたものです。

表 5-2 複製バージョン / 機能

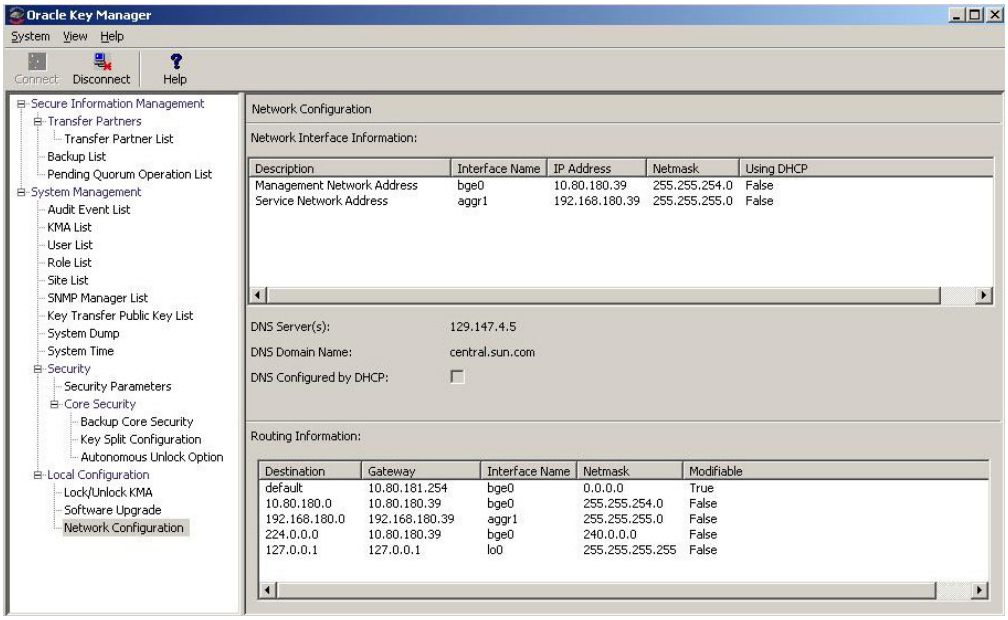
複製バージョン	KMS/OKM のバージョン	使用可能な機能
8	2.0	初期リリースに関連するすべての機能
9	2.0.2	バックアップ内の鍵 (バックアップに存在する使用可能な鍵)
10	2.1	IPv6 アドレス AES 鍵ラップ (FIPS モード)
11	2.2	ICSF 統合 分散定足数 SNMP プロトコルバージョン 2c
12	2.3	初期更新の高速化
13	2.4	エージェントのローミング

ネットワーク構成情報

「Network Configuration」メニューオプションは、現在の接続先である KMA のネットワーク構成設定を表示します。これらの設定は、347 ページの「OKM コンソールの使用法」で説明する設定画面で定義されます。

ネットワーク構成の表示

ネットワーク構成を表示するには、「Local Configuration」メニューから「**Network Configuration**」を選択します。「Network Configuration」画面が表示されます。



フィールドの説明は次のとおりです。

説明

関連する情報が、管理ネットワークアドレスとサービスネットワークアドレスのどちらに適用されるかが表示されます。

Interface Name

QuickStart プログラムで定義する、管理ネットワークまたはサービスネットワークのホスト名。

IP アドレス

管理ネットワークまたはサービスネットワークの IP アドレス。

ネットマスク

管理ネットワークまたはサービスネットワークのサブネットマスクアドレス。

DNS Server(s)

この KMA で使用する 1 つ以上の DNS ネームサーバー (ある場合)。

DNS Domain Name

この KMA で使用する DNS ドメイン (ある場合)。

DNS Configured by DHCP

これらの DNS 設定が DHCP によって暗黙に設定されたかどうかを示します。

Using DHCP

管理ネットワークまたはサービスネットワークで DHCP を使用するかどうかを示します。

Destination

この KMA からのネットワークトラフィックの宛先となるサブネット。

Gateway

管理ネットワークまたはサービスネットワークで、ネットワークトラフィックが経路指定されるゲートウェイ IP アドレス。

Modifiable

ゲートウェイ設定が変更可能かどうかを示します。自動的に設定されるゲートウェイは変更できません。

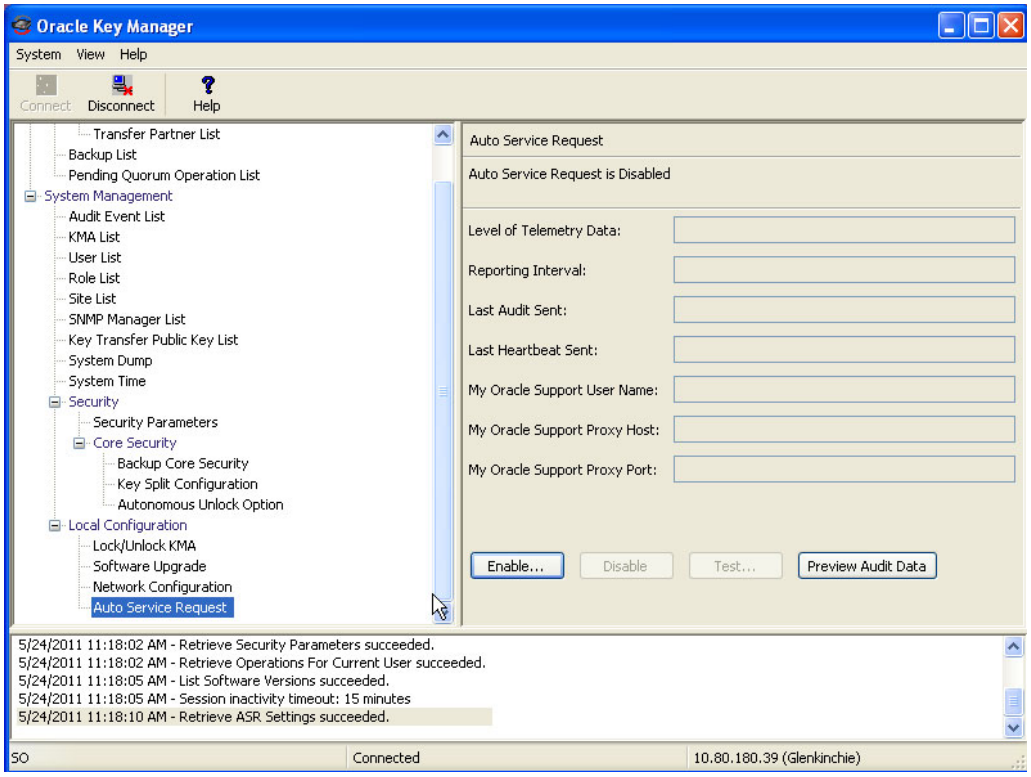
ASR (Auto Service Request)

ASR (Auto Service Request) 機能を使用して遠隔測定データを報告するように KMA を設定できます。KMA は定期的に、Oracle の遠隔測定 Web サイトに遠隔測定データを送信します。この KMA が Sun Fire X4170 M2 サーバーである場合、KMA は Integrated Lights Out Manager (ILOM) および Fault Management Architecture (FMA) 障害を送信して、発生する可能性があるハードウェア障害を報告することもできます。

ASR を使用可能にする

ASR 機能をオンに設定するには、次の手順を実行します。

1. 「Local Configuration」メニューから、「**Auto Service Request**」を選択します。



次に、フィールドとその説明を示します。

Level of Telemetry Data

この KMA が遠隔測定分析 Web サイトに送信する遠隔測定データのレベルが表示されます。取り得る値は次のとおりです。

- **Level 0** – 収集される、最小限の Solaris 固有の情報。
- **Level 1** – 発生しようとしているか、または発生している潜在的な問題があるかどうかを Oracle のサポート担当者が特定する際に役立つ可能性がある情報。
- **Level 2** – この KMA 上でどの OKM 機能が使用されているかについての詳細情報。

Reporting Interval

この KMA が遠隔測定データを遠隔測定分析 Web サイトに送信する頻度が表示されます。

Last Audit Sent

この KMA が遠隔測定データを遠隔測定分析 Web サイトに最後に送信した日時が表示されます。

Last Heartbeat Sent

この KMA がハートビートデータを遠隔測定分析 Web サイトに最後に送信した日時が表示されます。

My Oracle Support User Name

この KMA が資格情報として My Oracle Support サイトに提供するユーザー名が表示されます。

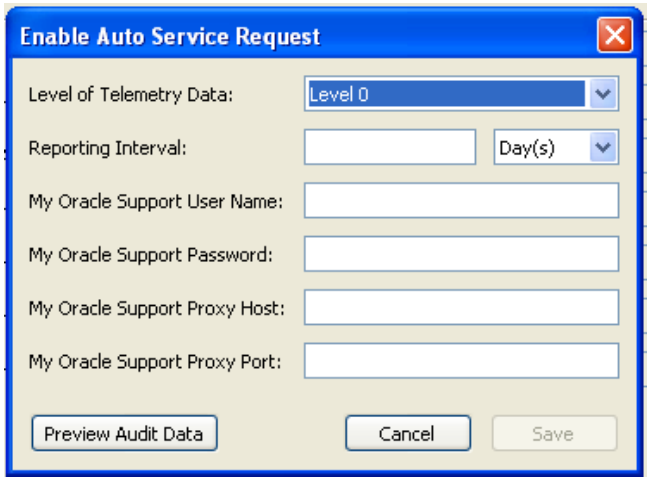
My Oracle Support Proxy Host

遠隔測定分析 Web サイトへの HTTPS 接続を確立するためにこの KMA が通信するプロキシホスト (ある場合) のネットワークアドレス (ホスト名または IP アドレス) が表示されます。

My Oracle Support Proxy Port

遠隔測定分析 Web サイトへの HTTPS 接続を確立するためにこの KMA が通信するプロキシホスト (ある場合) のプロキシポートが表示されます。

2. 「**Enable**」ボタンをクリックします。「**Enable Auto Service Request**」ダイアログボックスが表示されます。



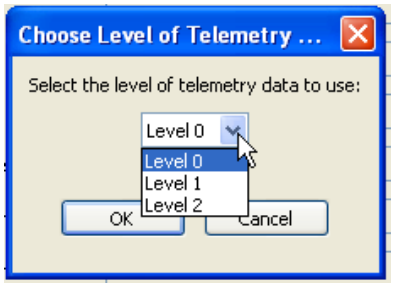
3. 遠隔測定データのレベルをドロップダウンから選択します。
4. 報告間隔を選択し、時間の単位をドロップダウンから選択します。

5. 次の情報を入力します。
    - My Oracle Support ユーザー名
    - My Oracle Support パスワード
    - My Oracle Support プロキシホスト (省略可能)
    - My Oracle Support プロキシポート (省略可能)

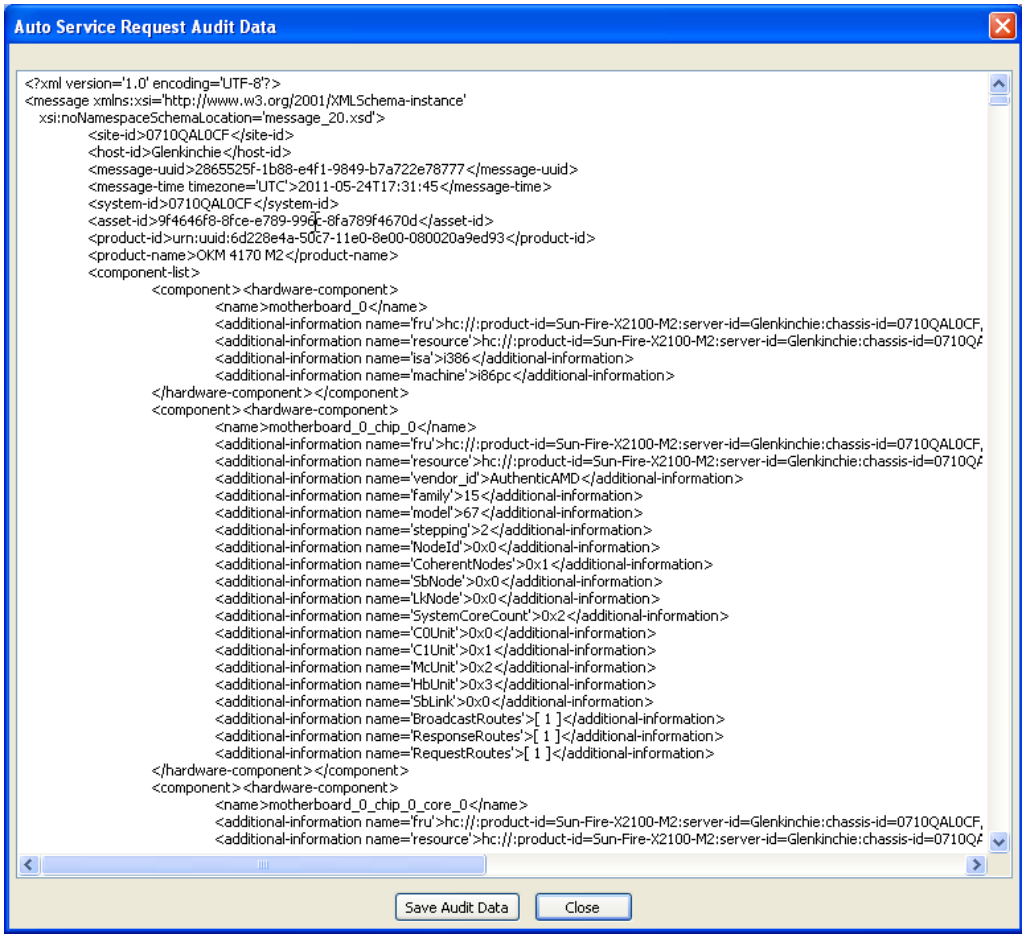
ASR 監査データのプレビュー

(適用前の場合も含めて) ASR 設定を入力したあとに、現在表示されている ASR 設定に基づいて遠隔測定分析サイトに送信される遠隔測定データを表示できます。データは実際には送信されません。

1. 遠隔測定データを表示するには、「**Preview Audit Data**」ボタンをクリックします。「**Choose Level of Telemetry Data**」ダイアログボックスが表示されます。



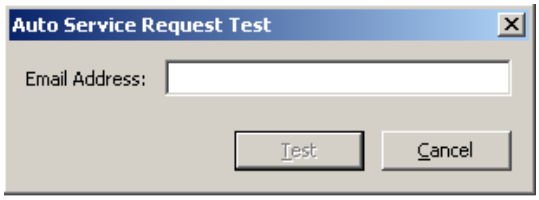
2. プレビューする遠隔測定データのレベルを選択して、「**OK**」ボタンをクリックします。「**Auto Service Request Audit Data**」ダイアログボックスに遠隔測定データが表示されます。



接続のテスト

ASR を使用可能にしたあとに、遠隔測定サイトへの接続をテストできます。「Local Configuration」メニュー (221 ページを参照) から、「**Auto Service Request**」を選択します。

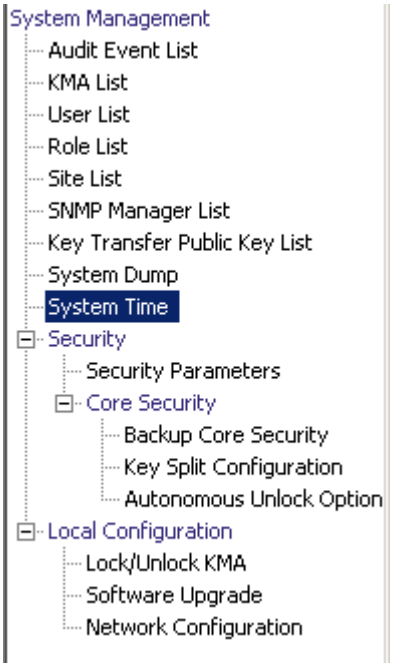
1. 「**Test**」ボタンをクリックします。「**Auto Service Request Test**」ダイアログが表示されます。



2. 電子メールアドレスを入力して「**Test**」ボタンをクリックします。
3. 電子メールアドレスをチェックし、遠隔測定サイトからのテスト電子メールメッセージを受信したかどうかを確認します。

「System Time」メニュー

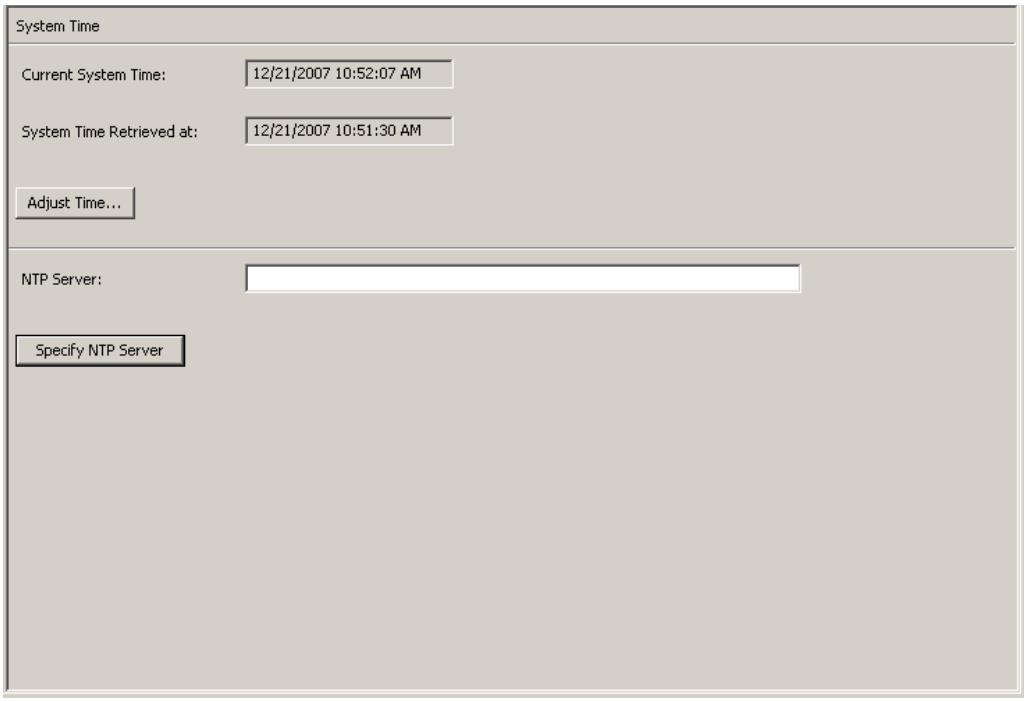
「System Time」メニューオプションを使用すると、接続しているシステムのクロックを設定できます。OKM ソリューションの正しい動作を保証するためには、クラスタ内の各 KMA が報告する時刻の差を 5 分以内に維持することが非常に重要です。



ローカルクロック情報の取得

ローカルクロック情報を取得するには、次の手順を実行します。

「System Management」メニューから、「**System Time**」を選択します。「System Time」画面が表示されます。



次に、フィールドとその説明を示します。

Current System Time

現在のシステム時刻が表示されます。

System Time Retrieved At

KMA のシステム時刻を取得したときのローカルクライアント時刻が表示されます。

Adjust Time

このボタンをクリックすると、システム時刻を変更できます。

KMA のクロックを変更する場合は、「Adjust Time」ボタンをクリックします。詳細は、「KMA のローカルクロックの調整」を参照してください。

NTP サーバー

この KMA が使用する NTP サーバーが表示されます (使用している場合)。

Specify NTP Server

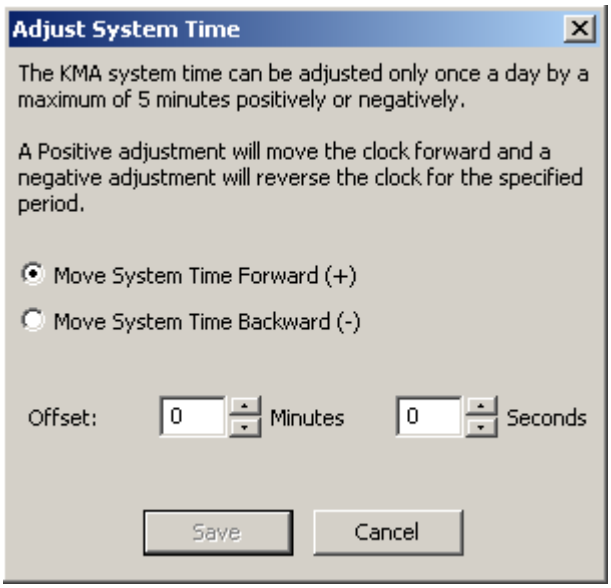
このボタンをクリックすると、この KMA で使用する NTP サーバーを指定できます。

KMA のローカルクロックの調整

KMA のクロックの調整では、1 日に一度だけ最大 5 分の範囲でクロックを進めるか、戻すことができます。正 (+) の調整では、クロックがゆっくりと先に進み、負 (-) の調整では、クロックがゆっくりと前に戻ります。

KMA のローカル時刻を調整するには、次の手順に従います。

1. 「System Time」メニューから、「**Adjust Time**」ボタンをクリックします。「Adjust System Time」ダイアログボックスが表示されます。



2. クロックに正の調整を行う場合は、「Move System Time Forward (+)」ラジオボタンを選択します。それ以外の場合は、「Move System Time Backward (-)」ラジオボタンを選択します。
3. 「Offset Minutes」テキストボックスで、数値を選択します。
4. 「Offset Seconds」テキストボックスで、数値を選択します。

   注 ー 指定した調整幅が大き過ぎるとエラーメッセージが表示され、より小さな値を入力するように求められます。「**OK**」ボタンをクリックしてこのダイアログボックスを閉じ、新しい値を入力します。

5. 「**Save**」ボタンをクリックして、変更を適用します。システムクロックが調整されます。

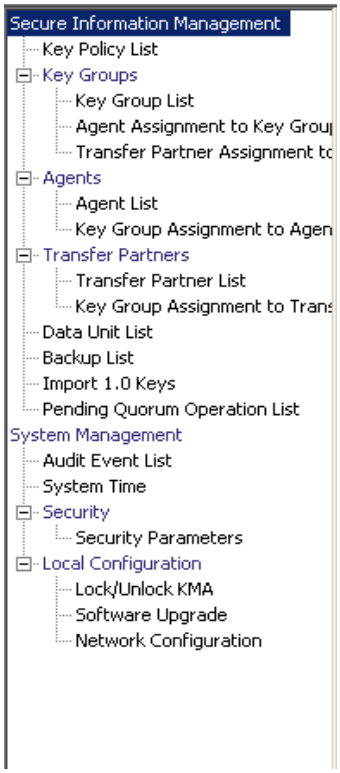
6

コンプライアンス責任者の操作

この章では、コンプライアンス責任者の役割が付与されたユーザーが実行できる操作について説明します。複数の役割が割り当てられている場合は、その役割を実行する手順について、該当する章を参照してください。

コンプライアンス責任者の役割

コンプライアンス責任者は、組織内のデータの流れを管理し、データコンテキスト (鍵グループ) と、データの保護方法および最終的な破棄方法を決定する規則 (鍵ポリシー) を定義および配備できます。これらの機能に対応するメニューは次のとおりです。



鍵ポリシー

鍵ポリシーは、データ管理に関する指針を提供します。OKM Manager では、鍵ポリシーを使用して、データの保護方法や破棄方法を決定します。鍵を作成してエージェントに提供するには、事前に鍵ポリシーを作成しておく必要があります。

鍵ポリシーを作成および変更できるのは、コンプライアンス責任者のみです。これによって、データが常にポリシーに準拠していることを確実にします。

「Key Policy List」メニュー

「Key Policies List」メニューでは、組織の鍵ポリシーを管理できます。

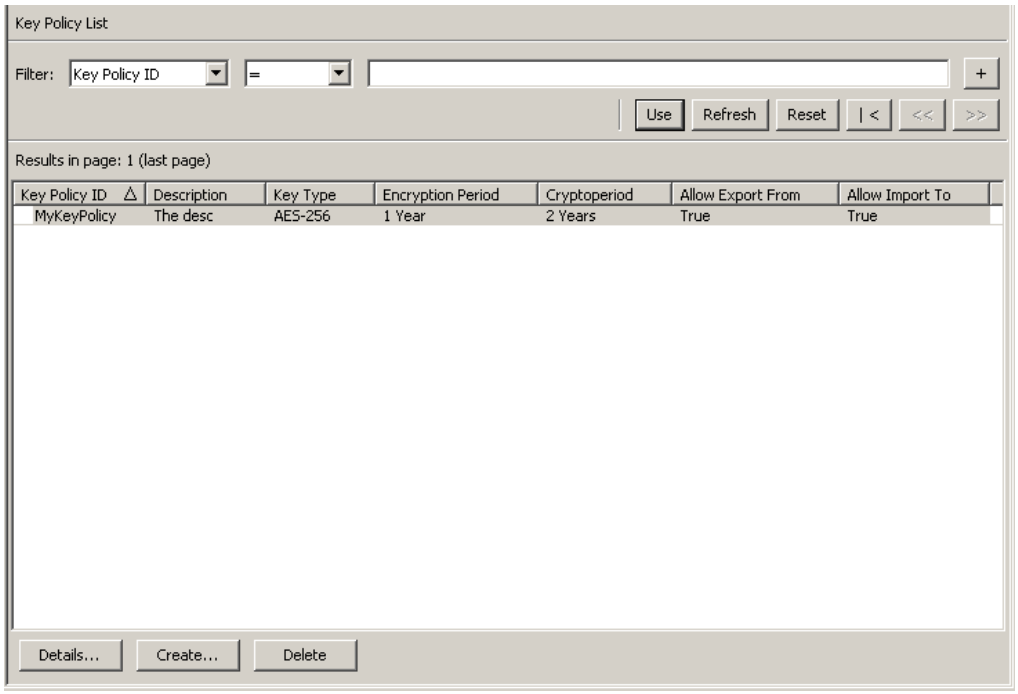
「Key Policy List」メニューオプションを使用すると、次の操作を行うことができます。

- 鍵ポリシーの表示
- 鍵ポリシーの詳細の表示および変更
- 鍵ポリシーの作成
- 既存の鍵ポリシーの削除

鍵ポリシーの表示

鍵ポリシーを表示するには、次の手順を実行します。

1. 「Secure Information Management」メニューから、「**Key Policy List**」を選択します。「Key Policy List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで鍵ポリシーリストにフィルタを適用することもできます。

- Key Policy ID
- 説明
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To

表示されている鍵ポリシーリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- Key Policy ID
- 説明
- Key Type
- Encryption Period
- Cryptoperiod
- Allow Export From
- Allow Import To

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス :

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用 :

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Key Policy ID

各鍵ポリシーを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。鍵ポリシー ID は、いったん作成すると変更できません。

説明

鍵ポリシーの説明が示されます。この値は、1 ～ 64 文字で指定できます。

Key Type

この鍵ポリシーに関連付けられている鍵で使用される暗号化アルゴリズムのタイプを示します。取り得る値は AES-256 だけです。

> **注 ー** 「Encryption Period」および「Cryptoperiod」は、鍵がはじめてエージェントに割り当てられた時点から開始します。ポリシーの「Encryption period」および「Cryptoperiod」は変更できません。これは、鍵ポリシーの変更が多数の鍵に影響することを回避するためです。

Encryption Period

この鍵ポリシーに関連付けられている鍵を、データの暗号化または復号化に使用できる期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Cryptoperiod

この鍵ポリシーに関連付けられている鍵を、データの復号化に使用できる (しかし暗号化には使用できない) 期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Allow Export From

この鍵ポリシーに関連付けられているデータユニット鍵をエクスポートできるかどうかを示します。True または False の値を取ります。

Allow Import To

この鍵ポリシーに関連付けられているデータユニット鍵をインポートできるかどうかを示します。True または False の値を取ります。

鍵ポリシーを作成する場合は、「**Create**」ボタンをクリックします。詳細については、246 ページの「鍵ポリシーの作成」を参照してください。

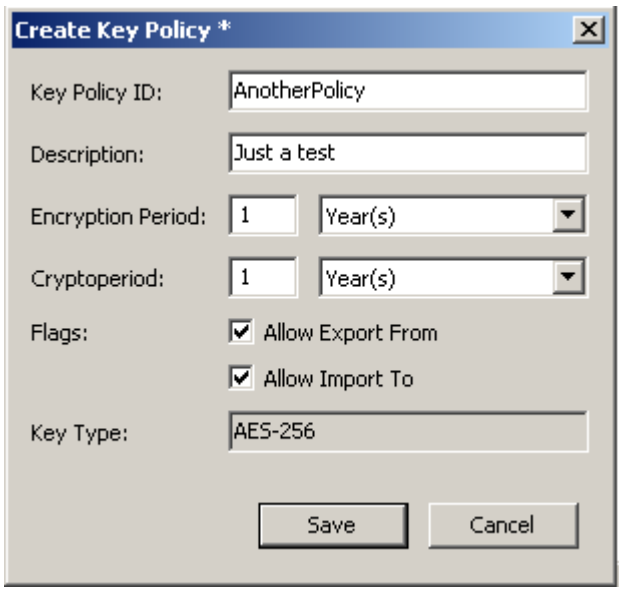
鍵ポリシーを表示または変更する場合は、その鍵ポリシーを強調表示して「**Details**」ボタンをクリックします。詳細については、248 ページの「鍵ポリシーの表示および変更」を参照してください。

鍵ポリシーを削除する場合は、「**Delete**」ボタンをクリックします。詳細については、249 ページの「鍵ポリシーの削除」を参照してください。

鍵ポリシーの作成

鍵ポリシーを作成するには、次の手順を実行します。

1. 「Key Policy List」画面から、「**Create**」ボタンをクリックします。「Create Key Policy」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

Key Policy ID

ポリシーを識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

説明

ポリシーを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

Encryption Period

この鍵ポリシーに関連付けられている鍵を、データの暗号化または復号化に使用できる期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

Cryptoperiod

この鍵ポリシーに関連付けられている鍵を、データの復号化に使用できる (しかし暗号化には使用できない) 期間が表示されます。時間間隔の単位は、分、時間、日、週、月、または年です。

フラグ

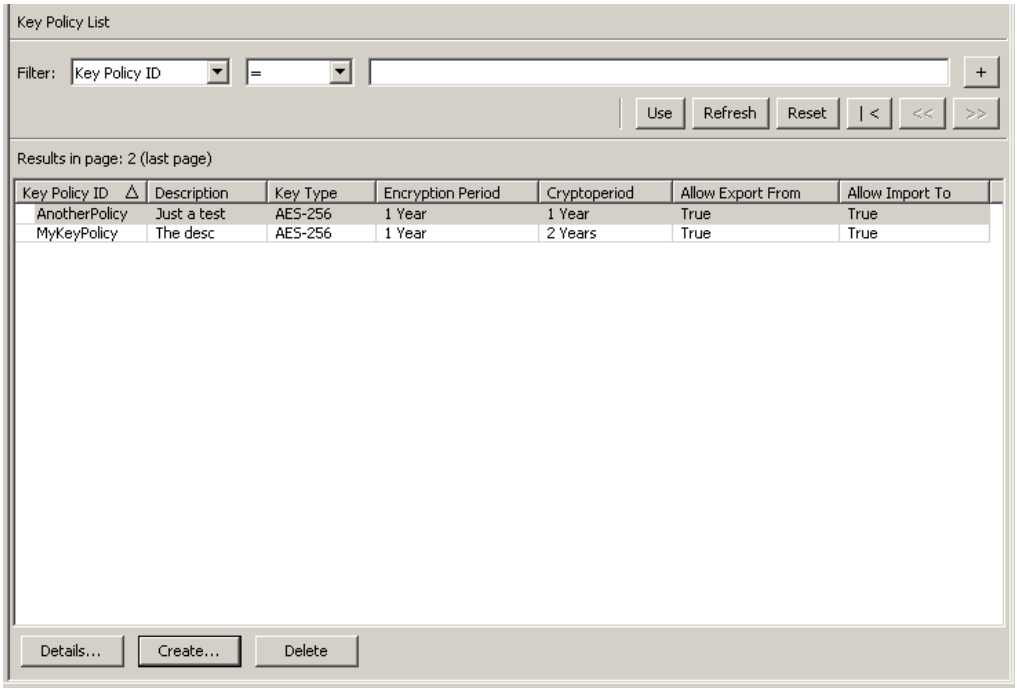
Allow Export From

この鍵ポリシーに関連付けられているデータユニット鍵をエクスポートできるかどうかを示します。True または False の値を取ります。

Allow Import To

この鍵ポリシーに関連付けられているデータユニット鍵をインポートできるかどうかを示します。True または False の値を取ります。

3. 「**Save**」ボタンをクリックして鍵ポリシーを保存します。「Key Policy List」画面に、新しい鍵ポリシーが表示されます。これで、この鍵ポリシーを鍵グループで使用できるようになります。

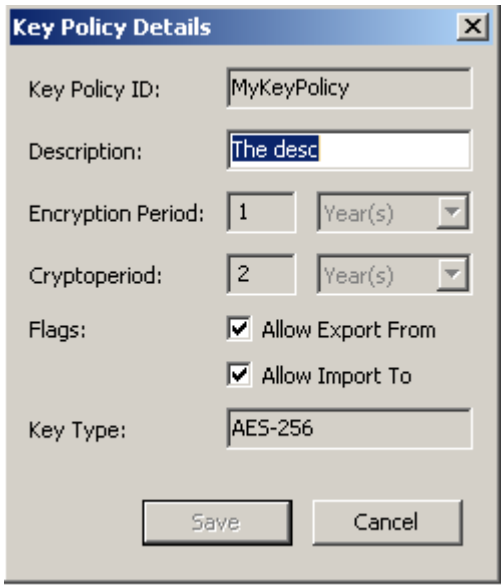


鍵ポリシーの表示および変更

注 ー 鍵ポリシーの詳細情報を表示できるのは、コンプライアンス責任者のみです。

鍵ポリシーの詳細を変更するには、次の手順を実行します。

1. 「Key Policy List」画面から、詳細情報を表示する鍵ポリシーをダブルクリックするか、またはその鍵ポリシーを強調表示して「**Details**」ボタンをクリックします。「Key Policy Details」ダイアログボックスが表示されます。



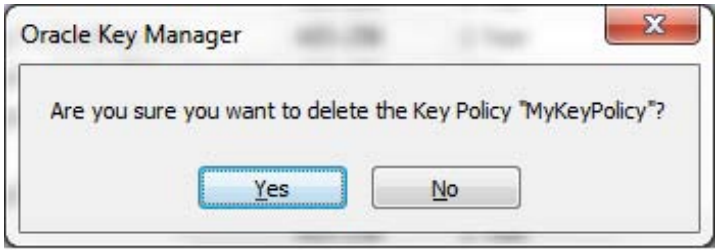
2. 必要に応じて、「`Description`」、「`Allow Export From`」、および「`Allow Import To`」フィールドを変更できます。終了したら、「**Save**」ボタンをクリックして変更内容を保存します。システムによって新しい鍵ポリシーの評価と妥当性検査が行なわれたあと、新しい鍵ポリシーに鍵グループが関連付けられます。
3. 「**Cancel**」ボタンをクリックした場合は、変更が保存されずにダイアログボックスが閉じます。

鍵ポリシーの削除

鍵ポリシーは、鍵グループまたは鍵で使用されていない場合にのみ削除できます。

鍵ポリシーを削除するには、次の手順を実行します。

1. 「Key Policy List」画面から、削除する鍵ポリシーを強調表示し、「**Delete**」ボタンをクリックします。次のように、指定した鍵ポリシーの削除を確認するダイアログボックスが表示されます。



2. 「Yes」ボタンをクリックして、鍵ポリシーを削除します。鍵ポリシーがデータベースから削除されます。「Key Policy List」画面に戻ります。リストから鍵ポリシーが削除されています。

鍵グループ

鍵グループとは、適用される鍵ポリシーとアクセスできるエージェントを決定するデータコンテキストです。鍵がエージェントに割り当てられ、データユニットのためにはじめて使用されると、その鍵は鍵グループに関連付けられます。鍵グループを作成するときには、鍵ポリシーを選択する必要があります。選択した鍵ポリシーが、その鍵グループ内の鍵に適用されます。

エージェントは鍵グループに関連付けられます。エージェントは、アクセスを許可された 1 つ以上の鍵グループを持ちます。エージェントは、アクセスを許可された鍵グループに属する鍵のみを取得できます。また、エージェントにデフォルトの鍵グループが存在することもあります。エージェントが新しい鍵を割り当てると、その鍵はそのエージェントのデフォルトの鍵グループに配置されます。エージェントが新しい鍵を割り当てることができるのは、そのエージェントにデフォルトの鍵グループが存在する場合だけです。

図 6-1 に、鍵グループ、鍵ポリシー、エージェント、およびデータユニットの関係を示します。

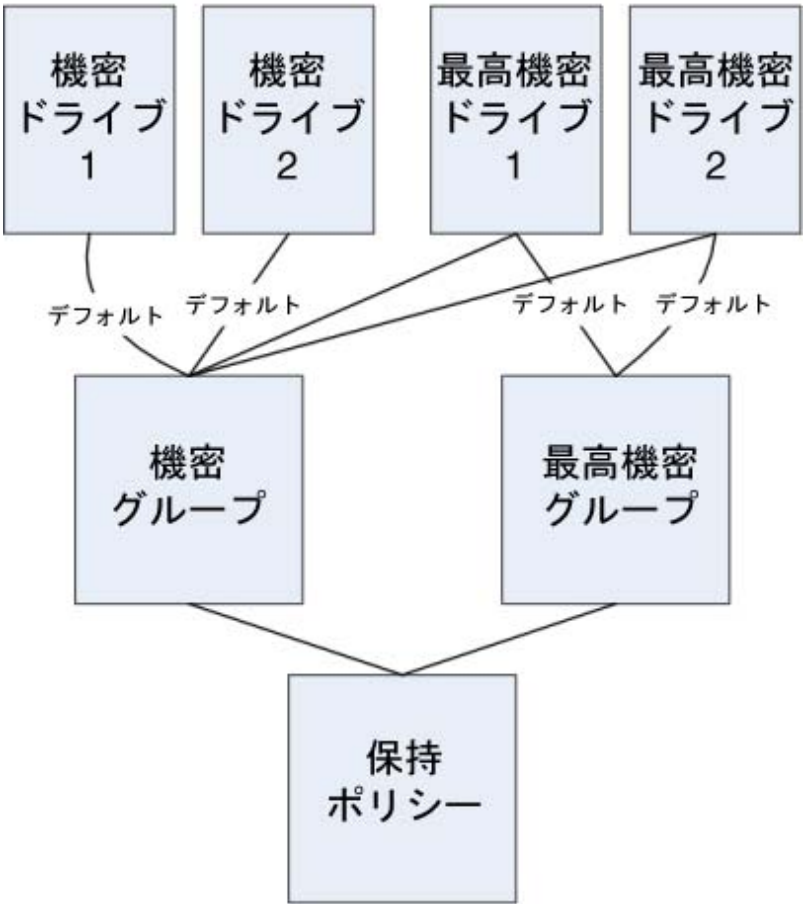
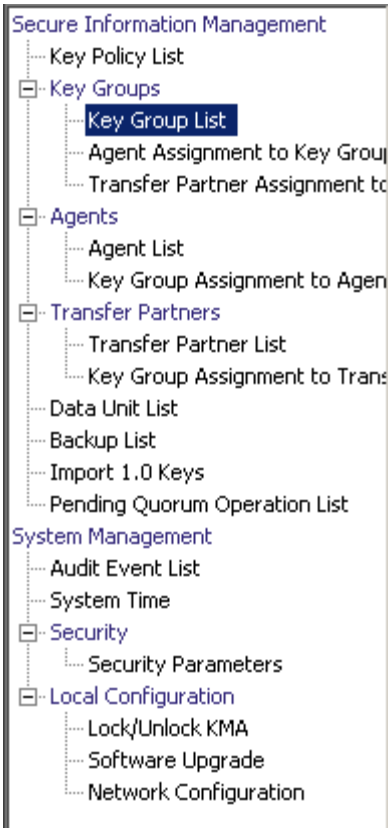


図 6-1 鍵グループと鍵ポリシー、エージェント、データユニットとの関係

「Key Groups」メニュー

「Key Groups」メニューに含まれている「Key Group List」メニューオプションを使用すると、コンプライアンス責任者は、鍵グループを管理できます。



「Key Group List」メニュー

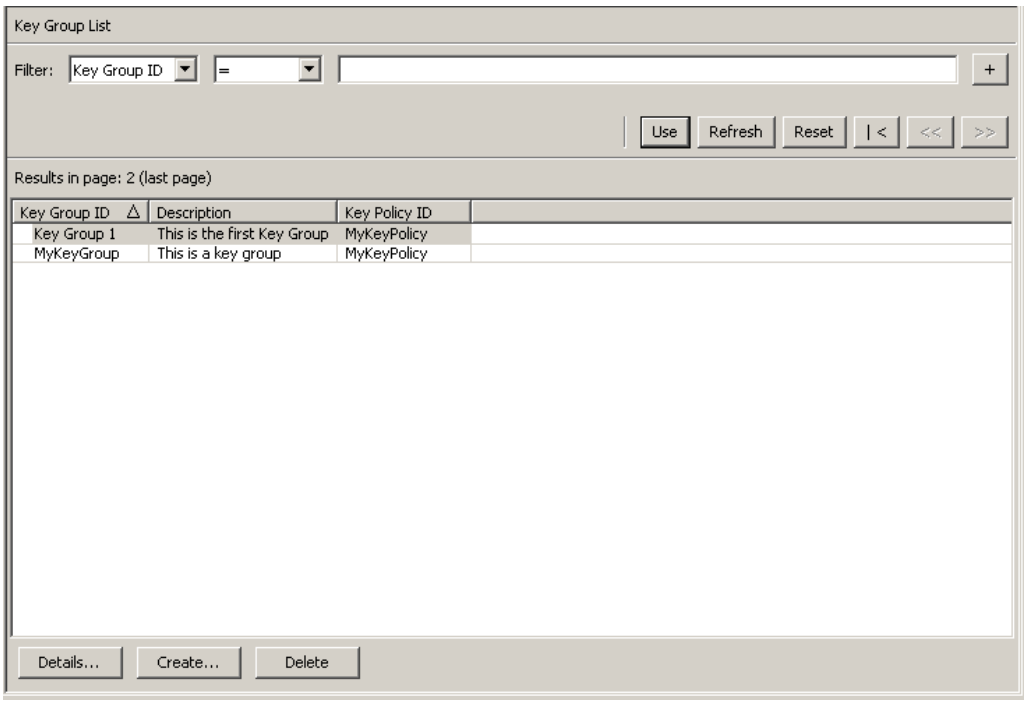
「Key Group List」メニューオプションを使用すると、次を行うことができます。

- 鍵グループの表示
- 鍵グループの作成
- 既存の鍵グループの変更
- 既存の鍵グループの削除

鍵グループの表示

すべての鍵グループを表示するには、次の手順を実行します。

「Key Groups」メニューから、「**Key Group List**」を選択します。「Key Group List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで鍵グループリストにフィルタを適用することもできます。

- Key Group ID
- 説明
- Key Policy ID

「**Use**」ボタンは、表示されている鍵グループのリストにフィルタを適用します。

次に、フィールドとその説明を示します。

フィルタ：

表示されている鍵グループのリストにフィルタを適用するためのフィルタオプションを選択します。すべてのフィルタを満たす鍵グループのみが表示されます。

フィルタ属性コンボボックス：

下矢印ボタンをクリックし、フィルタ条件として使用する属性を選択します。取り得る値は次のとおりです。

- Key Group ID
- 説明
- Key Policy ID

フィルタ演算子ボックス :

下矢印ボタンをクリックし、選択した属性に適用するフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス :

選択した属性のフィルタ条件として使用する値を入力します。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用 :

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、表示されているリストが再表示されます。この操作では、前回の「Use」または「Reset」操作以降に選択されたフィルタは適用されず、リストのページは変更されません。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

現在のページに表示できる項目数が表示されます。リストの最後の項目を表示している場合は、項目数に「(last page)」が付加されます。1 ページに表示する最大項目数は、「Options」ダイアログの「Query Page Size」値で定義されています。

Key Group ID

各鍵グループを識別する一意の識別子が表示されます。この値は、1 ～ 64 文字で指定できます。鍵グループ ID は、いったん定義すると変更できません。

説明

鍵グループの説明が示されます。この値は、1 ～ 64 文字で指定できます。

Key Policy ID

鍵グループ内の各データユニットに適用される既存の鍵ポリシーを識別する一意の識別子が表示されます。

既存の鍵グループの鍵ポリシー ID は変更できません。これは、変更が多数の鍵に影響することを回避するためです。

鍵グループを作成する場合は、「**Create**」ボタンをクリックします。詳細については、256 ページの「鍵グループの作成」を参照してください。

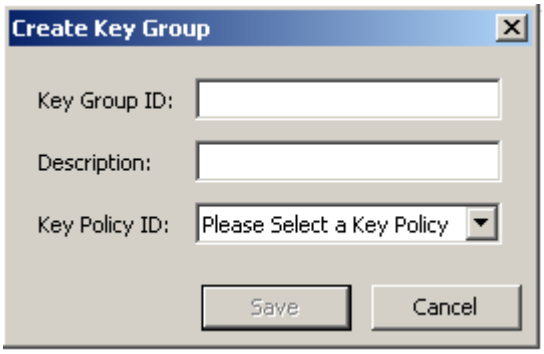
鍵グループを表示または変更する場合は、その鍵グループを強調表示して「**Details**」ボタンをクリックします。詳細については、258 ページの「鍵グループの詳細の表示および変更」を参照してください。

鍵グループを削除する場合は、「**Delete**」ボタンをクリックします。詳細については、259 ページの「鍵グループの削除」を参照してください。

鍵グループの作成

新しい鍵グループを作成するには、次の手順を実行します。

1. 「Key Group List」画面から、「**Create**」ボタンをクリックします。「Create Key Group」ダイアログボックスが表示されます。



2. 次のパラメータを設定します。

Key Group ID

鍵グループを識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

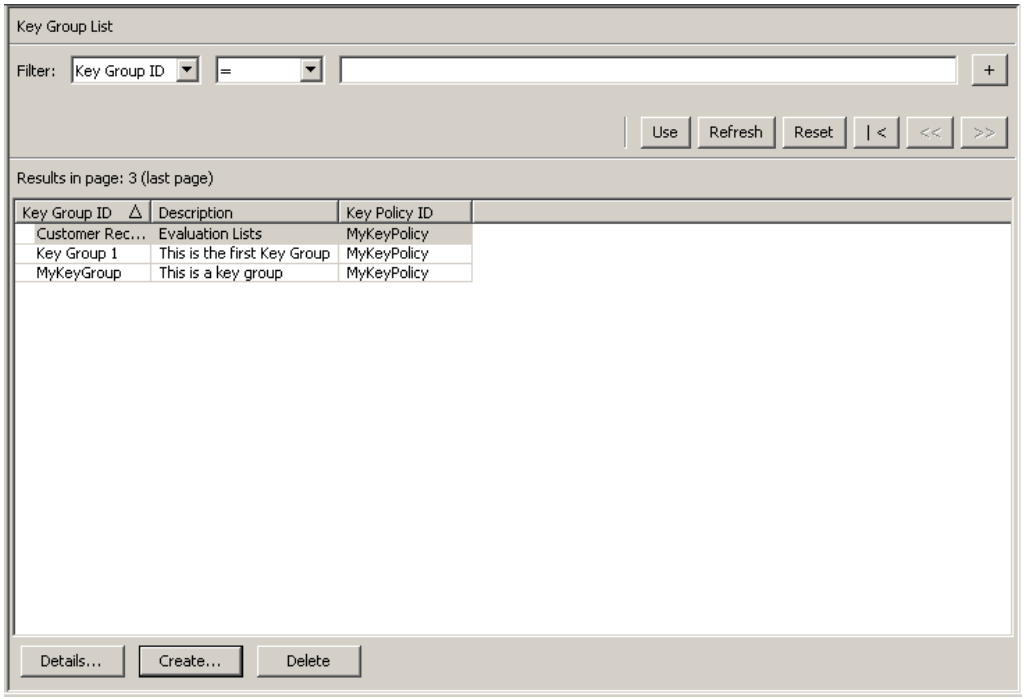
説明

鍵グループを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Key Policy ID

下矢印ボタンをクリックし、この鍵グループに関連付ける鍵ポリシーを選択します。新しい鍵グループを作成する場合は、既存の鍵ポリシーが表示されます。

3. 「**Save**」ボタンをクリックします。新しい鍵グループが作成されてデータベースに保存され、「Key Group List」画面に表示されます。これで、データユニット、エージェントなどで鍵グループを使用できるようになります。

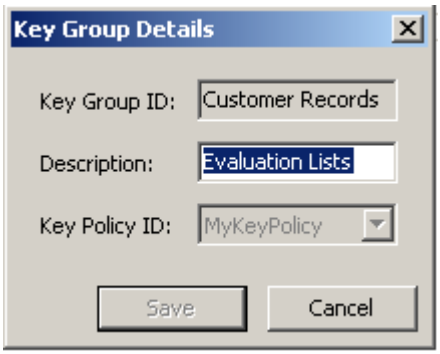

Key Group List
Filter:
Key Group ID
=
+
Use
Refresh
Reset
| <
<<
>>
Results in page: 3 (last page)
Key Group ID
Description
Key Policy ID
Customer Rec...
Evaluation Lists
MyKeyPolicy
Key Group 1
This is the first Key Group
MyKeyPolicy
MyKeyGroup
This is a key group
MyKeyPolicy
Details...
Create...
Delete

鍵グループの詳細の表示および変更

注 ー コンプライアンス責任者以外のユーザーが鍵グループの詳細情報を表示する場合は、「Save」ボタンを含むすべてのフィールドが使用不可になります。

鍵グループを変更するには、次の手順を実行します。

1. 「Key Group List」画面から、詳細情報を表示する鍵グループエントリをダブルクリックするか、またはその鍵グループエントリを強調表示して「**Details**」ボタンをクリックします。「Key Group Details」ダイアログボックスが表示されます。



次のパラメータが表示されます。

Key Group ID:

鍵グループを一意に識別します。このフィールドは読み取り専用です。

説明

鍵グループを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。このフィールドは、空白のままにすることができます。

Key Policy ID:

鍵グループおよび鍵グループ内のすべての鍵に関連付けられている既存の鍵ポリシーを識別する一意の識別子が表示されます。このフィールドは読み取り専用です。

2. 変更できるのは「Description」フィールドのみです。終了したら、「**Save**」ボタンをクリックして変更内容を保存します。「Key Group List」画面に戻ります。

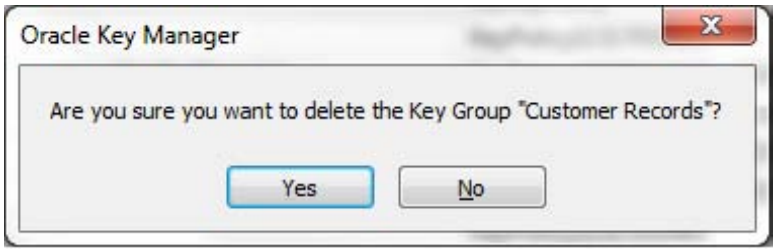
鍵グループの削除

注 ー アクティブな鍵グループ、つまりエージェントまたはデータユニットが割り当てられている鍵グループは削除できません。

鍵グループを削除するには、次の手順を実行します。

1. 「Key Groups List」画面から、削除する鍵グループを強調表示し、「**Delete**」ボタンをクリックします。次の「Confirmation」ダイアログボックスが表示され、選択された鍵グループを削除することを確認するよう求められます。

   鍵グループは、鍵で使用されておらず、エージェントにも関連付けられていない場合にのみ削除できます。

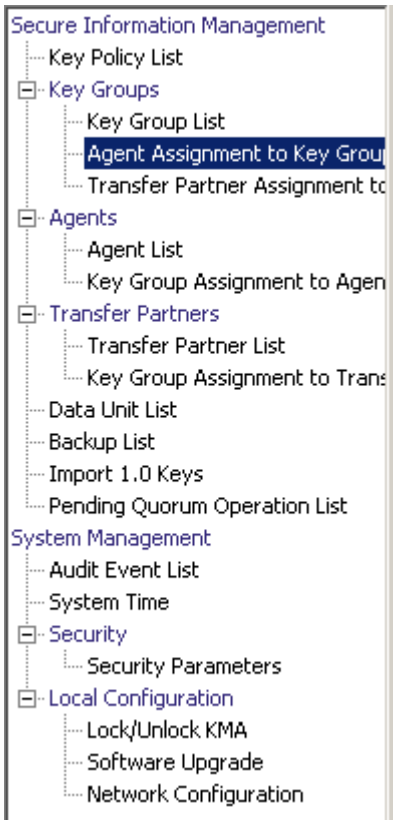


2. 「**Yes**」ボタンをクリックして、鍵グループを削除します。鍵グループと、それに関連付けられたエントリが、データベースから削除されます。「Key Group List」画面に戻ります。リストから鍵グループが削除されています。

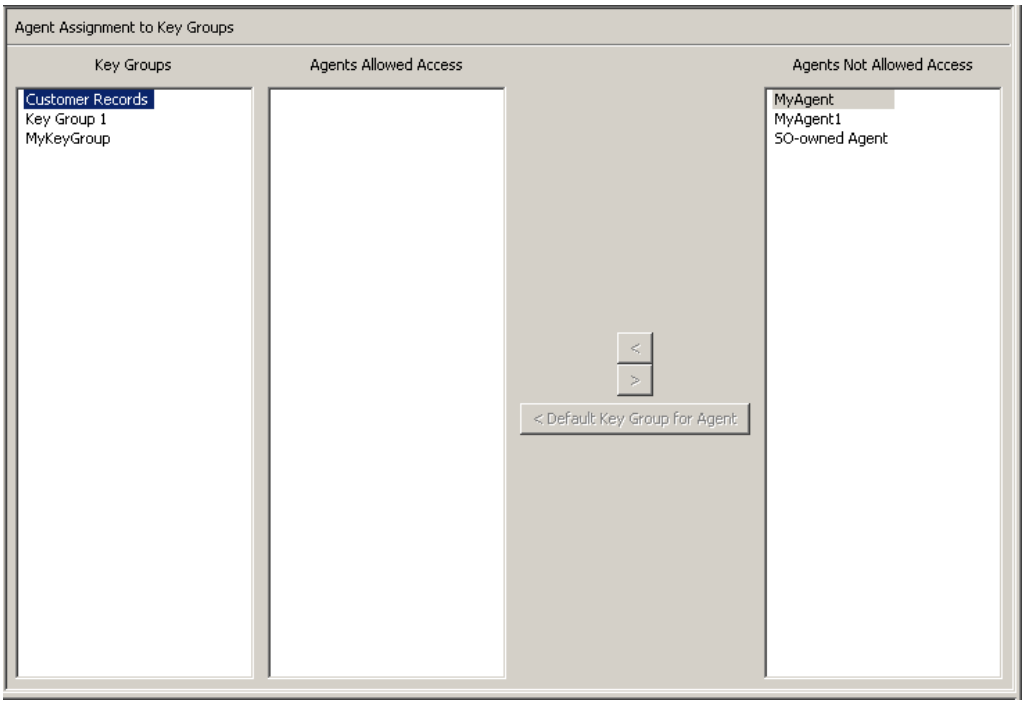
「Agent Assignment to Key Groups」メニュー

「Agent Assignment to Key Groups」メニューオプションを使用すると、エージェントを鍵グループに割り当てることができます。エージェントを鍵グループに割り当てることで、そのエージェントがアクセスできるストレージデバイスが決定されます。これは「Agents」メニューの「Key Group Assignment」メニューオプションの逆の操作ですが、どちらも結果は同じになります。

重要 ― エージェントによる鍵の割り当てを可能にするには、事前にそのエージェントのデフォルトの鍵グループを設定しておく必要があります。



エージェントの割り当てを表示するには、「Key Groups」メニューから「**Agent Assignment to Key Groups**」を選択します。「Agent Assignment to Key Groups」画面が表示されます。

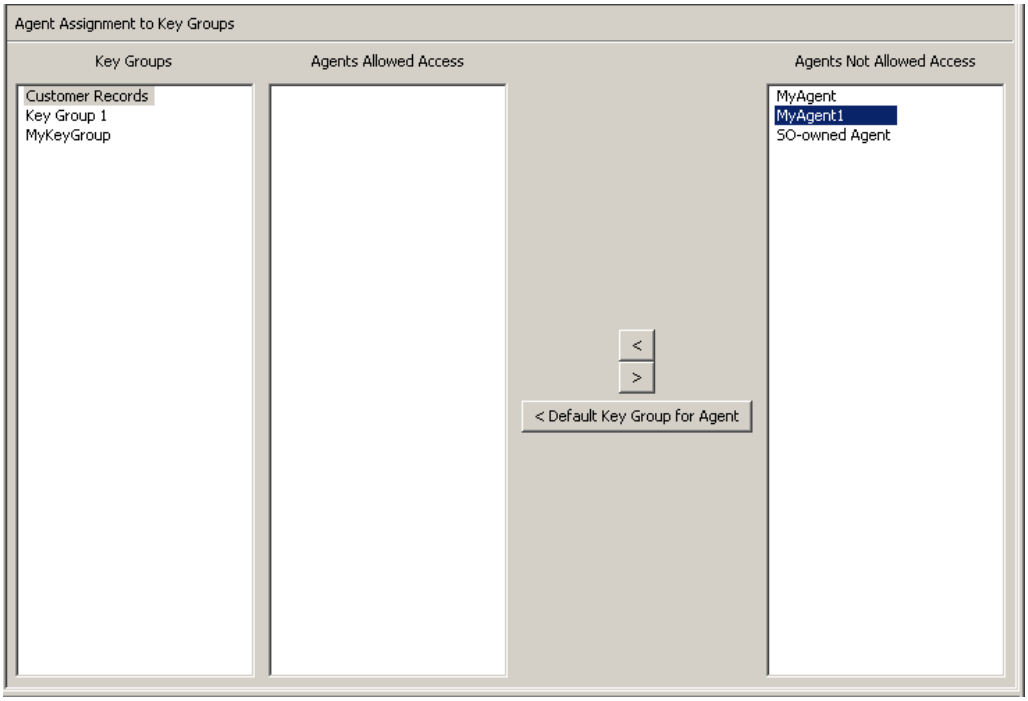


「Key Groups」列に、鍵グループが一覧表示されます。「Agents Allowed Access」列に、選択した鍵グループに割り当てられているエージェントが一覧表示されます。「Agents Not Allowed Access」列に、選択した鍵グループに割り当てられていないエージェントが一覧表示されます。

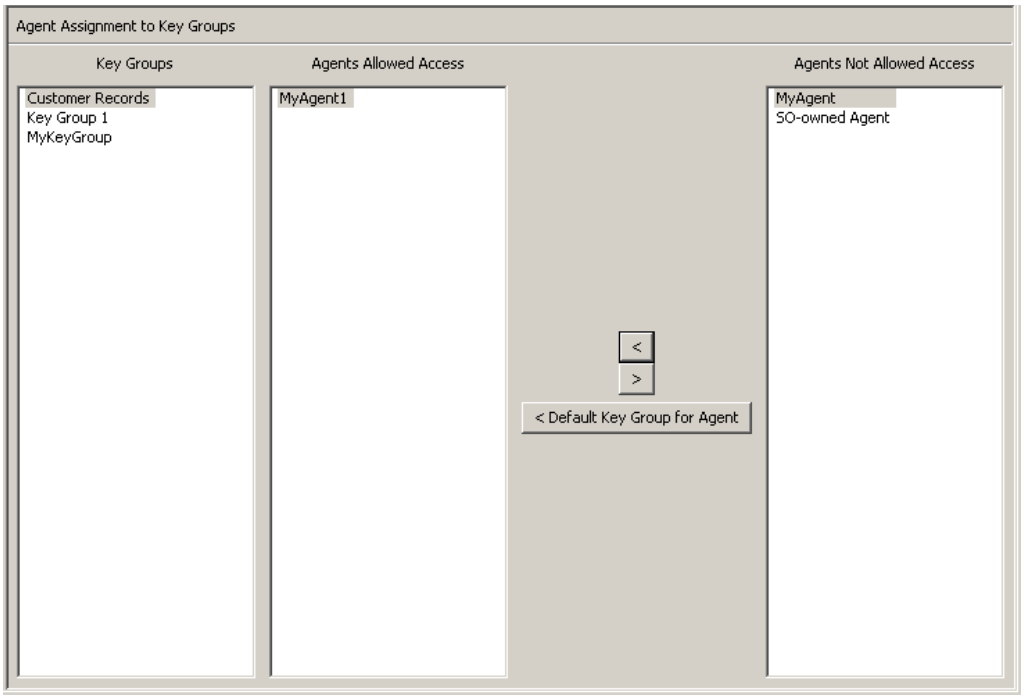
鍵グループへのエージェントの割り当て

鍵グループにエージェントを割り当てるには、次の手順を実行します。

1. 「Key Groups」列で、必要な鍵グループを強調表示します。「Agents Not Allowed Access」列で、追加するエージェントを強調表示し、「Move to  」ボタンをクリックします。



2. 選択したエージェントが「Agents Allowed Access」列に移動して、選択した鍵グループのエージェントリストにエージェントが正常に追加されたことを示します。



エージェントを鍵グループに割り当て、デフォルトの鍵グループを設定するには、次の手順を実行します。

1. 「Agent Assignment to Key Groups」画面で、「Key Groups」リストから必要な鍵グループを選択します。
2. 「Agents Not Allowed Access」リストで、追加してデフォルトの鍵グループを設定するエージェントを 1 つ以上選択します。
3. 「**Default Key Group for Agent**」ボタンをクリックします。選択したエージェントが「Agents Allowed Access」リストに移動して、その鍵グループにデフォルトの鍵グループが設定されます。これにより、エージェントは鍵グループにアクセスできるようになります。

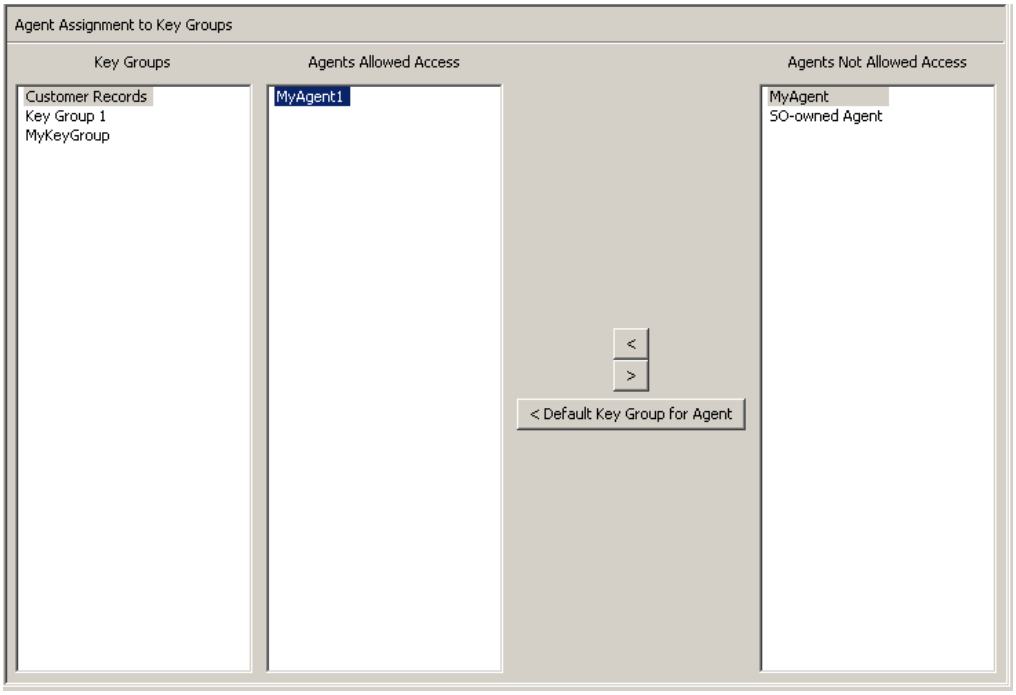
すでに割り当てられているエージェントに対してデフォルトの鍵グループを設定するには、次の手順を実行します。

1. 「Agent Assignment to Key Groups」画面で、「Key Groups」リストから必要な鍵グループを選択します。
2. 「Agents Allowed Access」リストで、デフォルトの鍵グループとして選択した鍵グループを持たない 1 つ以上のエージェントを選択します。
3. 「**Default Key Group for Agent**」ボタンをクリックします。選択されたエージェントのデフォルトの鍵グループが、その鍵グループに設定されます。

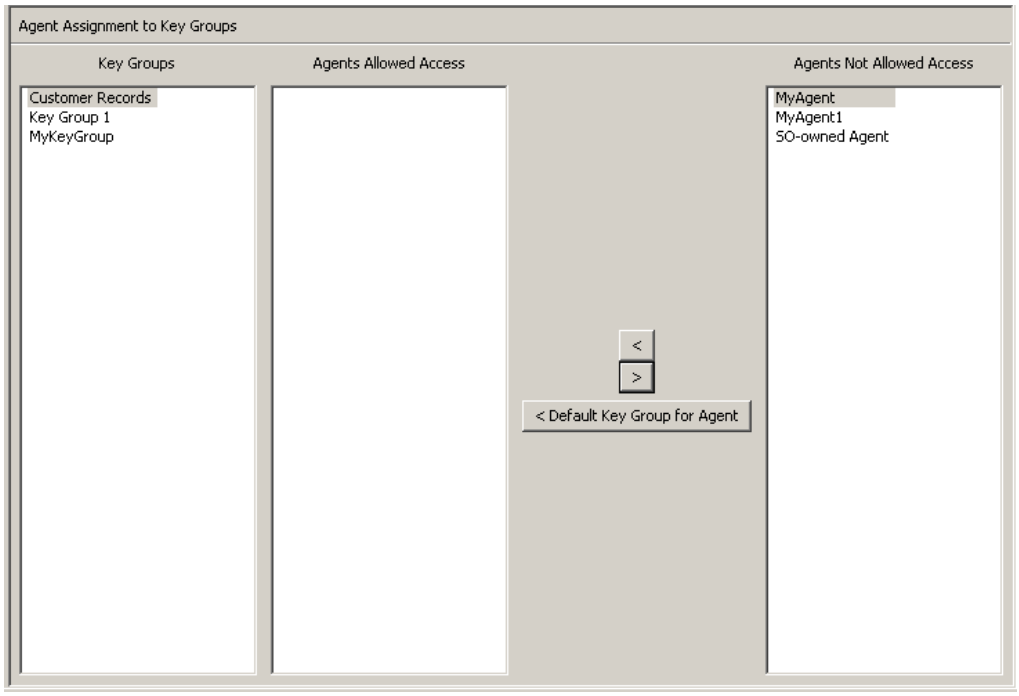
鍵グループからのエージェントの削除

鍵グループのエージェントリストからエージェントを削除するには、次の手順を実行します。

1. 「Key Groups」列で、必要な鍵グループを強調表示します。「Agents Allowed Access」列で、削除するエージェントを強調表示し、「Move from [>]」ボタンをクリックします。

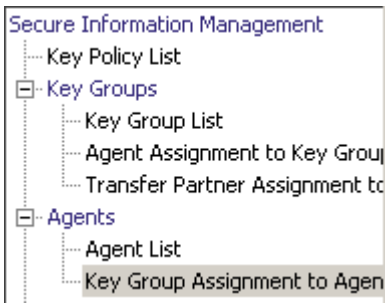


2. 選択したエントリが「Agents Allowed Access」列から削除され、「Agents Not Allowed Access」列に表示されます。選択した鍵グループへの割り当ては解除されています。


Agent Assignment to Key Groups
Key Groups
Agents Allowed Access
Agents Not Allowed Access
Customer Records
Key Group 1
MyKeyGroup
MyAgent
MyAgent1
SO-owned Agent
<
>
< Default Key Group for Agent

「Key Group Assignment to Agents」メニュー

「Key Group Assignment to Agents」メニューオプションを使用すると、鍵グループをエージェントに割り当てることができます。これは「Agent Assignment to Key Groups」メニューオプションの逆の操作ですが、どちらも結果は同じになります。

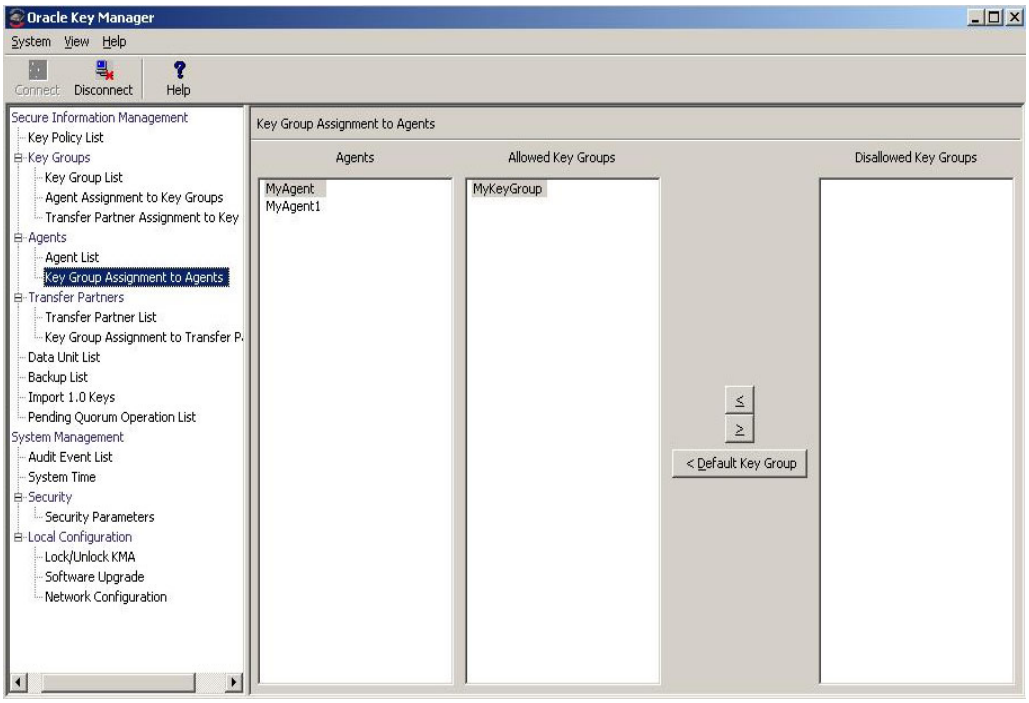


鍵グループを表示するには、次の手順を実行します。

1. 「Agents」メニューから「**Key Group Assignment**」を選択します。「Key Group Assignment to Agents」画面が表示されます。

「Agents」列に、データベース内のエージェントが一覧表示されます。「Allowed Key Groups」列に、エージェントがアクセスできる鍵グループが一覧表示されます。「Disallowed Key Groups」列に、エージェントがアクセスできない鍵グループが一覧表示されます。

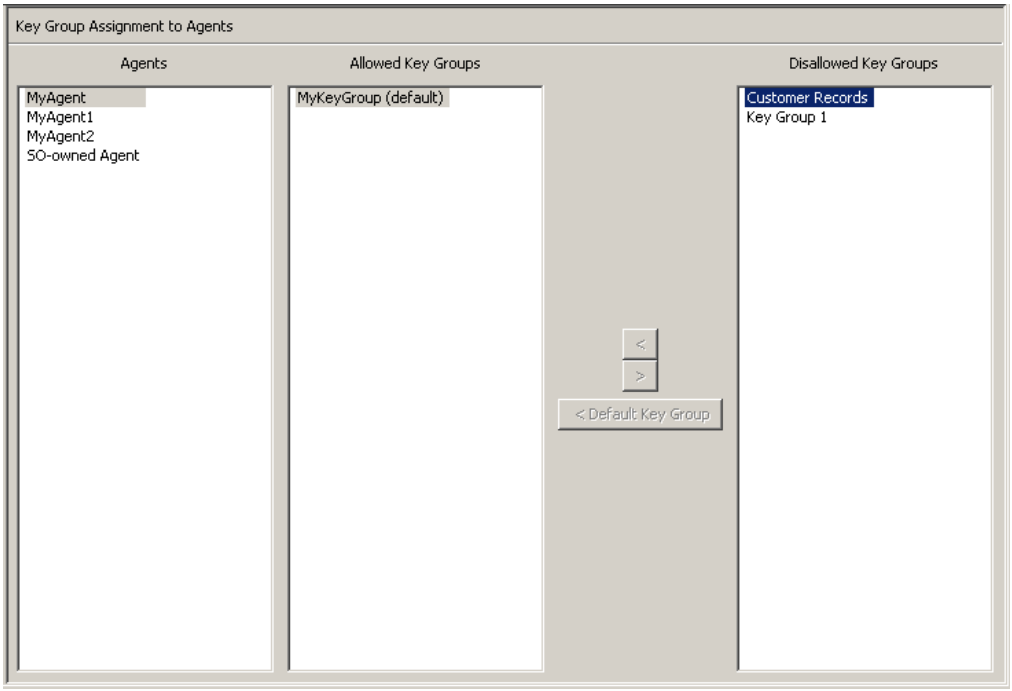
2. エージェントエントリをクリックすると、選択したエージェントのメンバーの鍵グループまたはメンバーでない鍵グループが表示されます。


Oracle Key Manager
System View Help
Connect Disconnect Help
Secure Information Management
Key Policy List
Key Groups
Key Group List
Agent Assignment to Key Groups
Transfer Partner Assignment to Key
Agents
Agent List
Key Group Assignment to Agents
Transfer Partners
Transfer Partner List
Key Group Assignment to Transfer P
Data Unit List
Backup List
Import 1.0 Keys
Pending Quorum Operation List
System Management
Audit Event List
System Time
Security
Security Parameters
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration
Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyKeyGroup
≤
≥
< Default Key Group

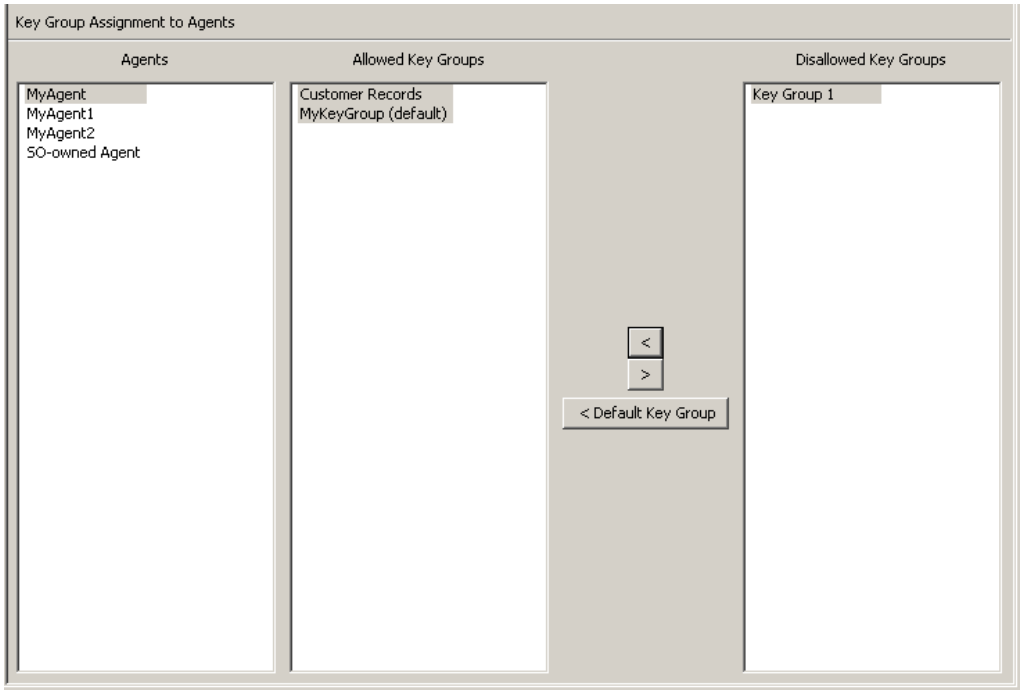
エージェントへの鍵グループの割り当て

エージェントに鍵グループを割り当てるには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」列で、必要なエージェントを強調表示します。「Disallowed Key Groups」列で、追加する鍵グループを強調表示し、「Move to <」ボタンをクリックします。



2. 選択したエントリが「Allowed Key Groups」列に移動し、選択したエージェントに鍵グループが正常に追加されます。



鍵グループをデフォルトの鍵グループとしてエージェントに割り当てるには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」リストで、必要なエージェントを選択します。
2. 「Disallowed Key Groups」リストで、追加してデフォルトの鍵グループとして設定する鍵グループを 1 つ選択します。
3. 「**Default Key Group**」ボタンをクリックします。選択した鍵グループが「Allowed Key Groups」リストに移動し、エージェントのデフォルトの鍵グループとして設定されます。これにより、エージェントは鍵グループにアクセスできるようになります。

すでに割り当てられている鍵グループをデフォルトの鍵グループに設定するには、次の手順を実行します。

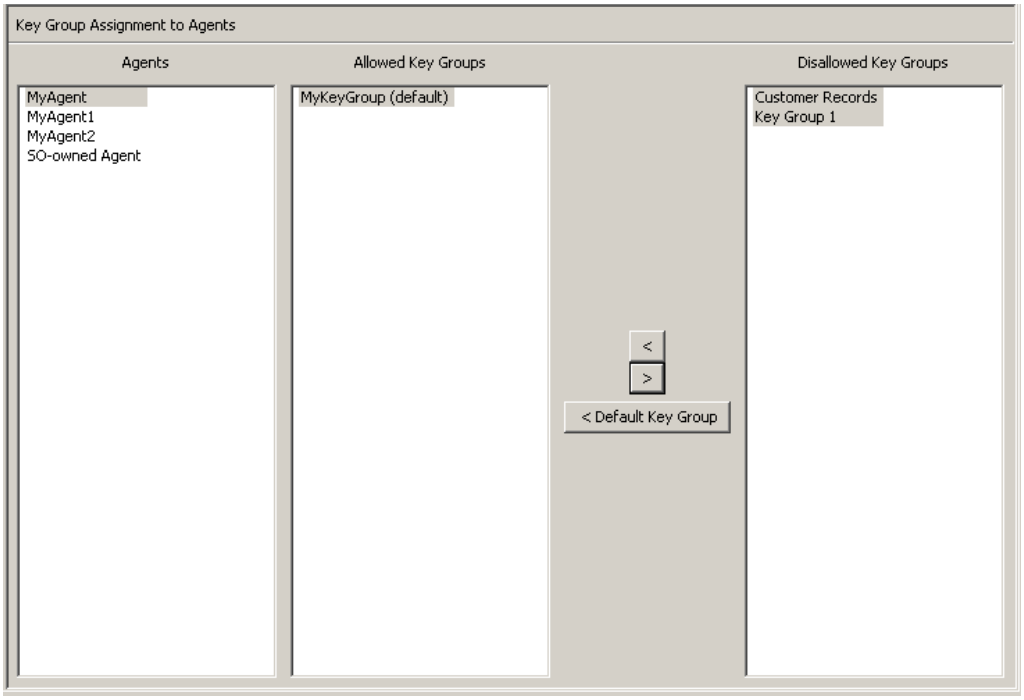
1. 「Key Group Assignment to Agents」画面の「Agents」リストで、必要なエージェントを選択します。
2. 「Allowed Key Groups」リストで、エージェントのデフォルトの鍵グループになっていない鍵グループを 1 つ選択します。

「**Default Key Group**」ボタンをクリックします。エージェントのデフォルトの鍵グループが、選択された鍵グループに設定されます。

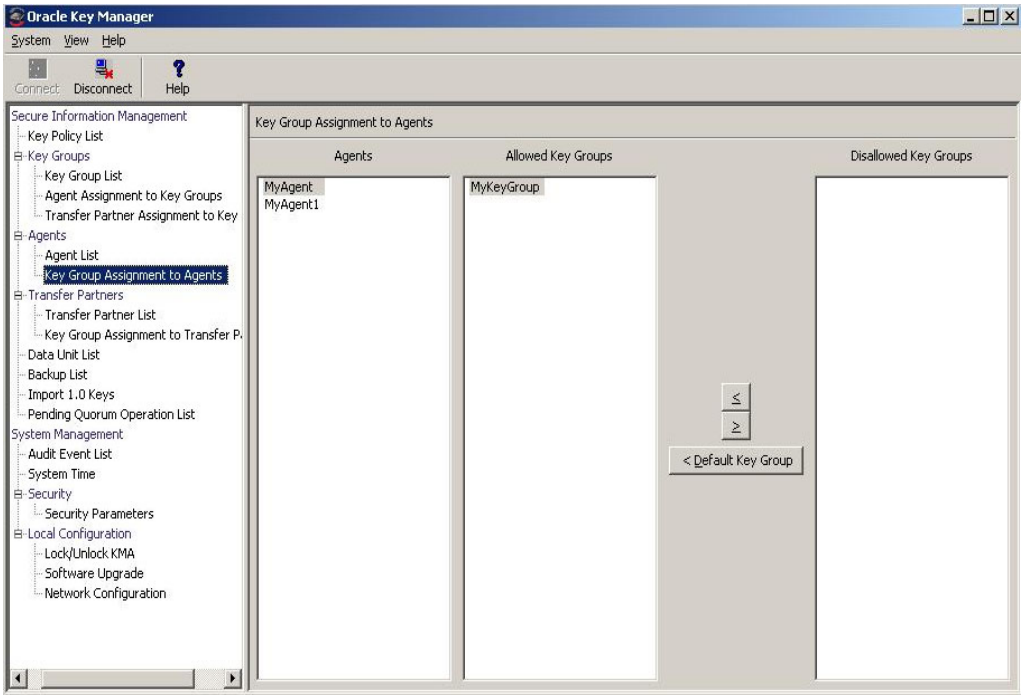
エージェントからの鍵グループの削除

エージェントから鍵グループを削除するには、次の手順を実行します。

1. 「Key Group Assignment to Agents」画面の「Agents」列で、必要なエージェントを強調表示します。「Allowed Key Groups」列で、削除する鍵グループを強調表示し、「Move from [>]」ボタンをクリックします。

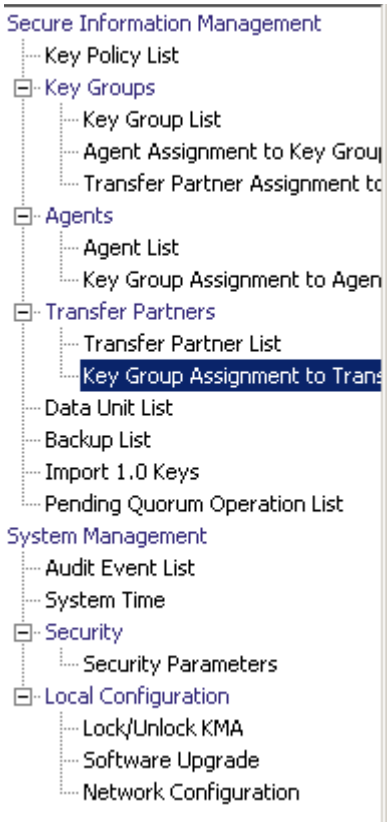


2. 選択されたエントリが「Allowed Key Groups」列から「Non-member of Info. Groups」列に移動され、エージェントに割り当てられた状態ではなくなります。


Oracle Key Manager
System View Help
Connect Disconnect Help
Secure Information Management
Key Policy List
Key Groups
Key Group List
Agent Assignment to Key Groups
Transfer Partner Assignment to Key
Agents
Agent List
Key Group Assignment to Agents
Transfer Partners
Transfer Partner List
Key Group Assignment to Transfer P.
Data Unit List
Backup List
Import 1.0 Keys
Pending Quorum Operation List
System Management
Audit Event List
System Time
Security
Security Parameters
Local Configuration
Lock/Unlock KMA
Software Upgrade
Network Configuration
Key Group Assignment to Agents
Agents
Allowed Key Groups
Disallowed Key Groups
MyAgent
MyAgent1
MyKeyGroup
≤
≥
< Default Key Group

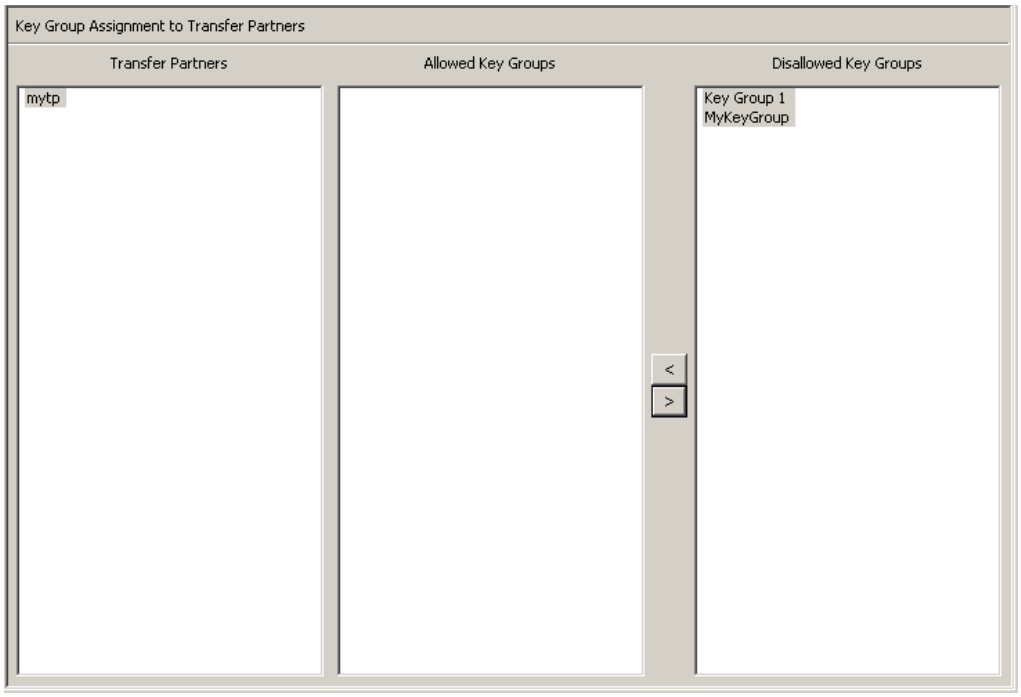
「Key Group Assignment to Transfer Partners」メニュー

「Key Group Assignment to Transfer Partners」メニューオプションを使用すると、鍵グループを転送パートナーに割り当てることができます。



鍵グループ割り当ての表示

鍵グループの割り当てを表示するには、「Transfer Partners」メニューから「**Key Group Assignment to Transfer Partners**」を選択します。次の画面が表示されます。

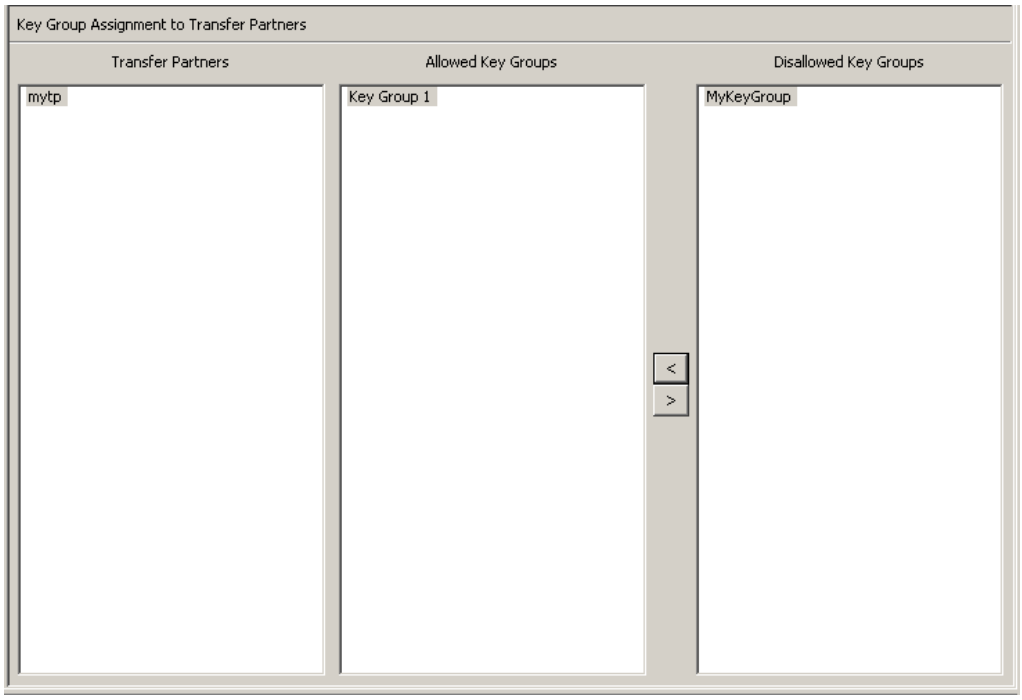


画面に、転送パートナーにアクセスできる鍵グループが表示されます。「Allowed Key Groups」列に、選択した転送パートナーに割り当てられた鍵グループが一覧表示されます。「Disallowed Key Groups」列に、転送パートナーに割り当てられていない鍵グループが表示されます。

転送パートナーへの鍵グループの追加

転送パートナーリストに鍵グループを追加するには、次の手順を実行します。

1. 「Transfer Partners」列で、対象とする転送パートナーを強調表示します。「Disallowed Key Groups」列で、追加する鍵グループを強調表示し、「Move to <」ボタンをクリックします。

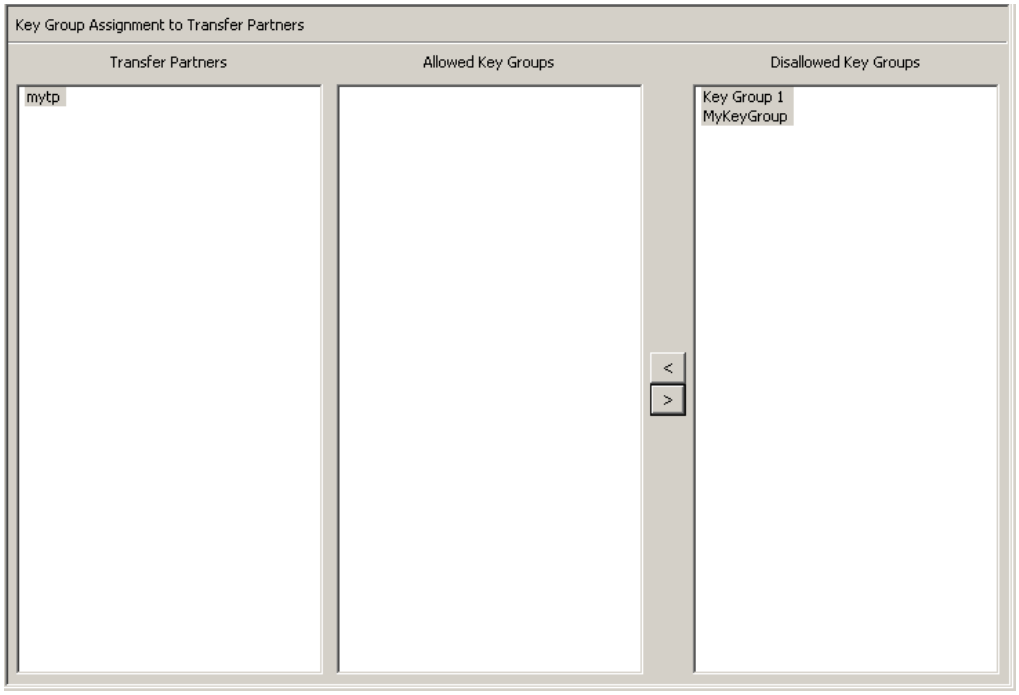


2. 選択した鍵グループが「Allowed Key Groups」列に移動して、転送パートナーがその鍵グループにアクセスできるようになったことを示します。

転送パートナーからの鍵グループの削除

転送パートナーから鍵グループリストを削除するには、次の手順を実行します。

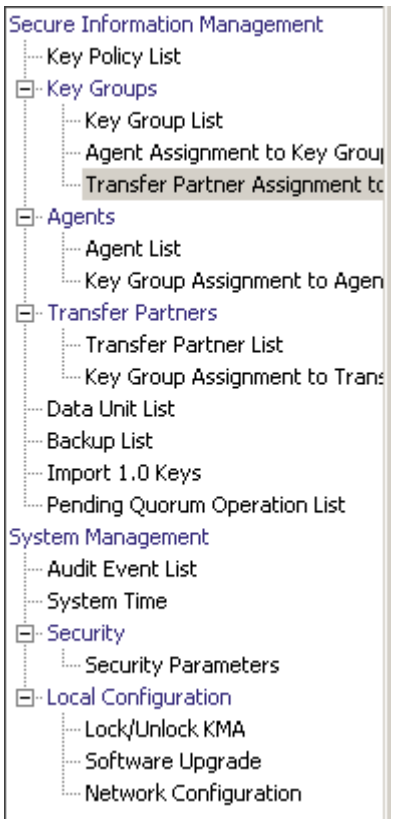
1. 「Transfer Partners」列で、対象とする転送パートナーを強調表示します。「Allowed Key Groups」列で、削除する鍵グループを強調表示し、「Move from >」ボタンをクリックします。



2. 選択した鍵グループが「Disallowed Key Groups」列に移動して、転送パートナーがその鍵グループにアクセスできなくなったことを示します。

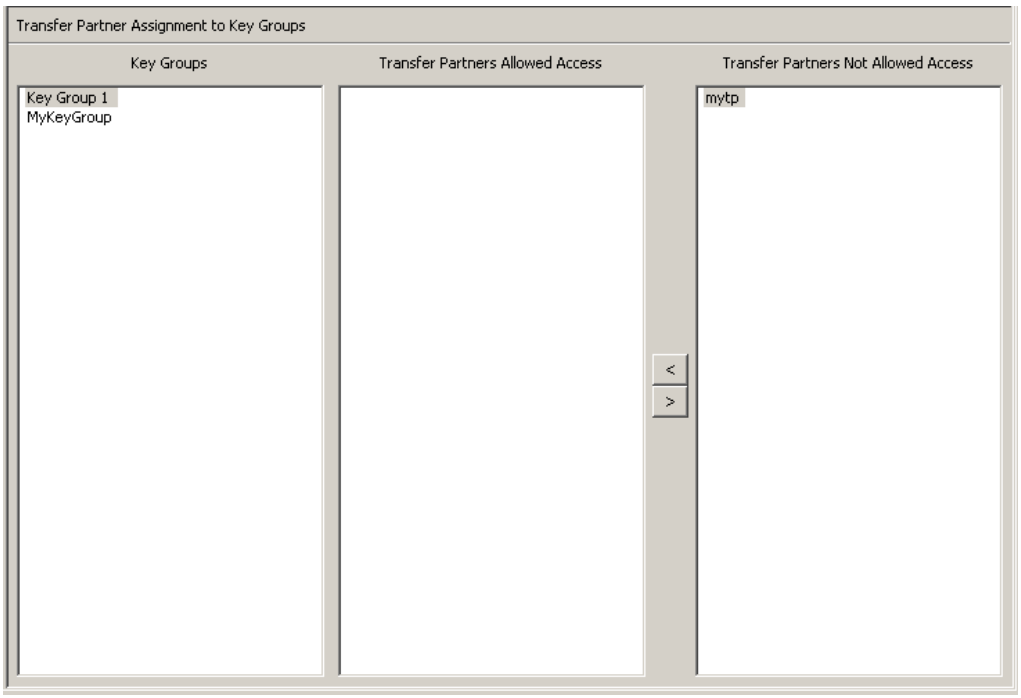
「Transfer Partner Assignment to Key Groups」メニュー

「Transfer Partner Assignment to Key Groups」メニューを使用すると、特定の鍵グループへのアクセスを許可されている一連の鍵転送パートナーに鍵転送パートナーを追加できます。



転送グループ割り当ての表示

転送グループ割り当てを表示するには、「Key Groups」メニューから「Transfer Partner Assignment to Key Groups」を選択します。次の画面が表示されます。

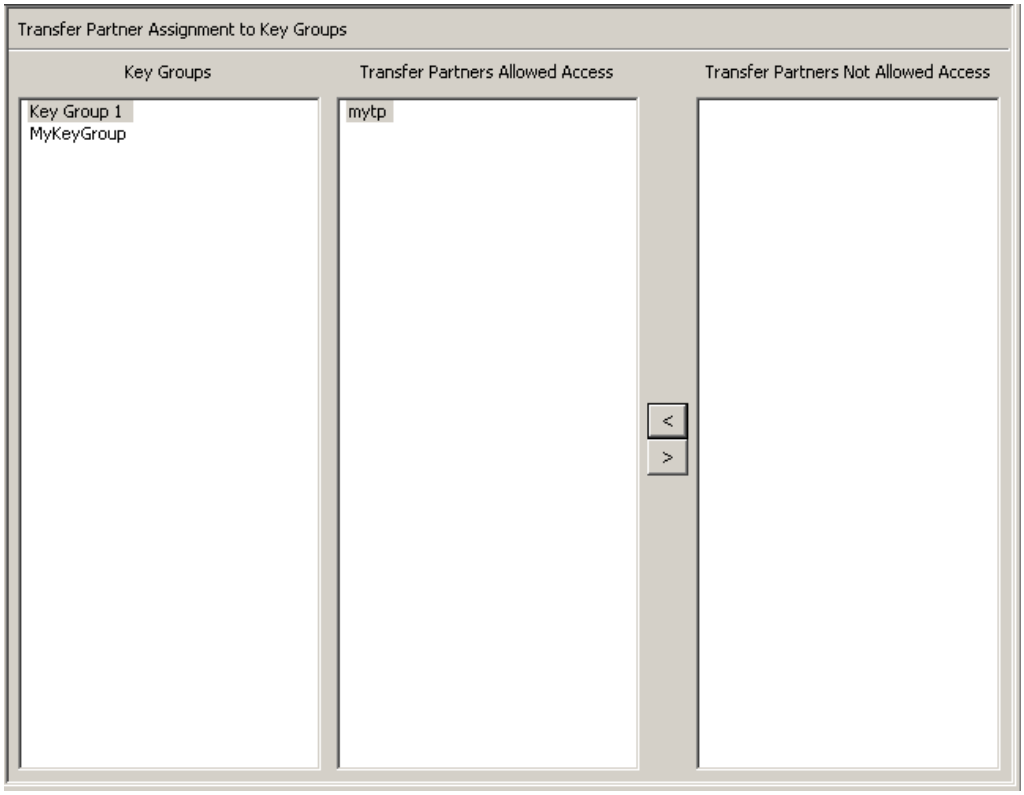


画面には、鍵グループにアクセスできる転送パートナーが表示されます。「Transfer Partners Allowed Access」列に、鍵グループに割り当てられている転送パートナーが一覧表示されます。「Transfer Partners Not Allowed Access」列に、鍵グループに割り当てられていない転送パートナーが表示されます。

鍵グループへの転送パートナーの追加

鍵グループに転送パートナーを追加するには、次の手順を実行します。

1. 「Key Groups」列で、対象とする鍵グループを強調表示します。「Transfer Partners Allowed Access」列で、追加する鍵グループを強調表示し、「Move to <」ボタンをクリックします。

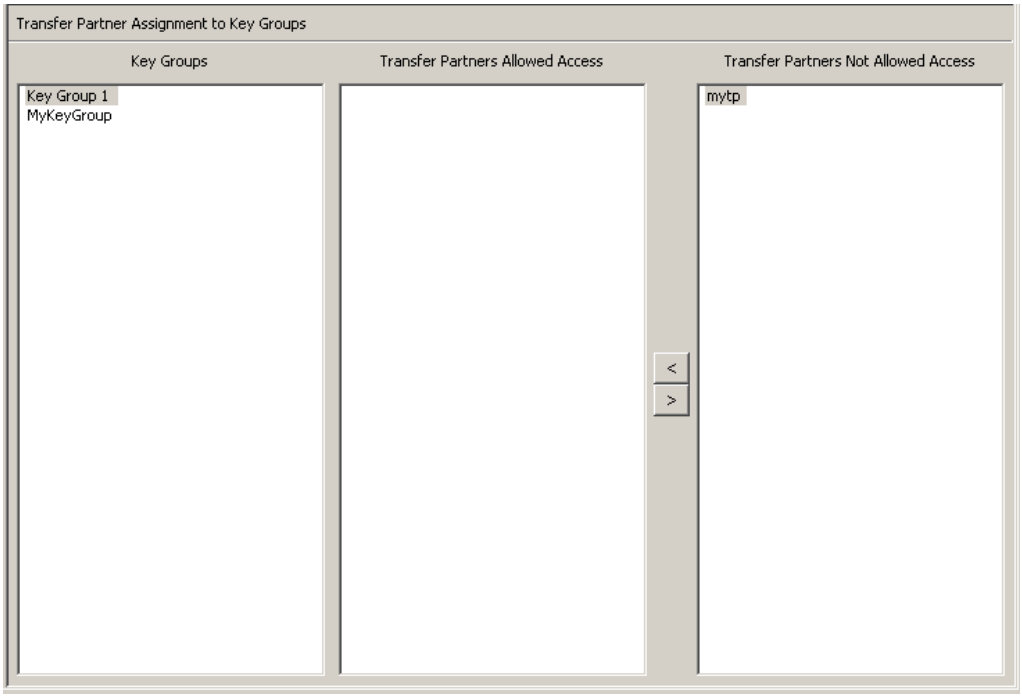


2. 選択した転送パートナーが「Transfer Partners Allowed Access」列に移動して、鍵グループがその転送パートナーにアクセスできるようになったことを示します。

鍵グループからの転送パートナーの削除

鍵グループから転送パートナーを削除するには、次の手順を実行します。

1. 「Key Groups」列で、対象とする鍵グループを強調表示します。「Transfer Partners Allowed Access」列で、削除する転送パートナーを強調表示し、「Move from >」ボタンをクリックします。

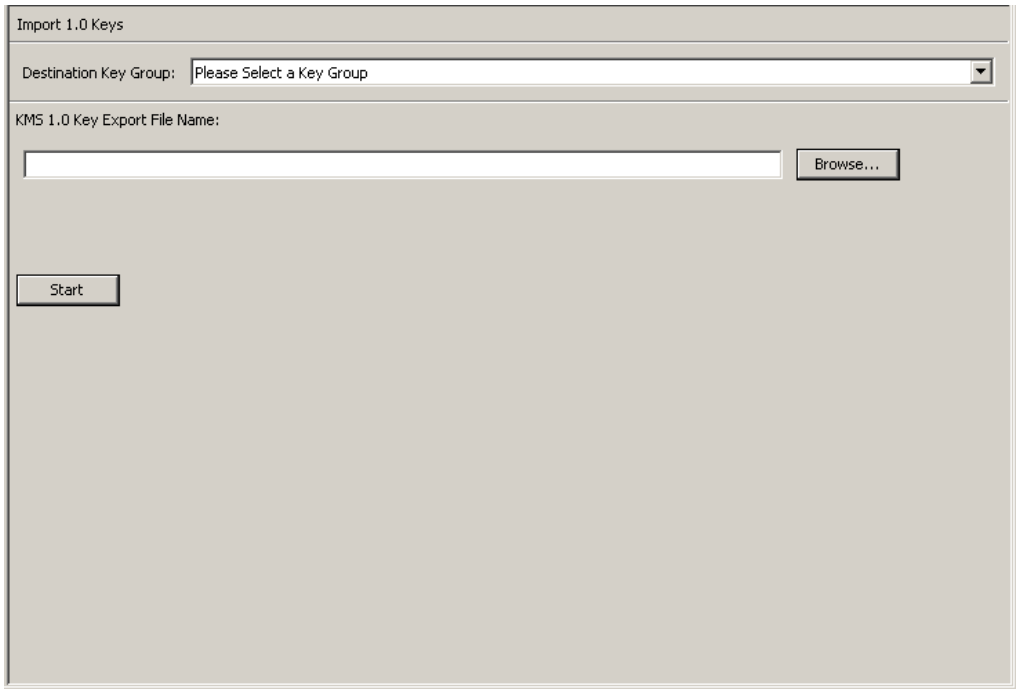


2. 選択した転送パートナーが「Transfer Partners Not Allowed Access」列に移動して、鍵グループがその転送パートナーにアクセスできなくなったことを示します。

KMS 1.0 の鍵エクスポートファイルのインポート

KMS 1.0 の鍵エクスポートファイルを KMA にインポートし、このファイル内の各鍵に対して新しい鍵を作成するには、次の手順を実行します。

1. KMS 1.2 システムに移動し、鍵をファイルにエクスポートします。インポートできるのは、KMS 1.2 システムからエクスポートされた鍵のみです。KMS 1.0 および 1.1 のシステムは、鍵をエクスポートする前に KMS 1.2 にアップグレードする必要があります。
2. 「Secure Information Management」メニューから「Import 1.0 Keys」を選択します。



3. 次のパラメータを設定します。

Destination Key Group

これらの鍵のインポート先となる鍵グループを選択します。

KMS 1.0 Key Export File Name

KMS 1.0 の鍵エクスポートファイルの名前を入力します。

参照

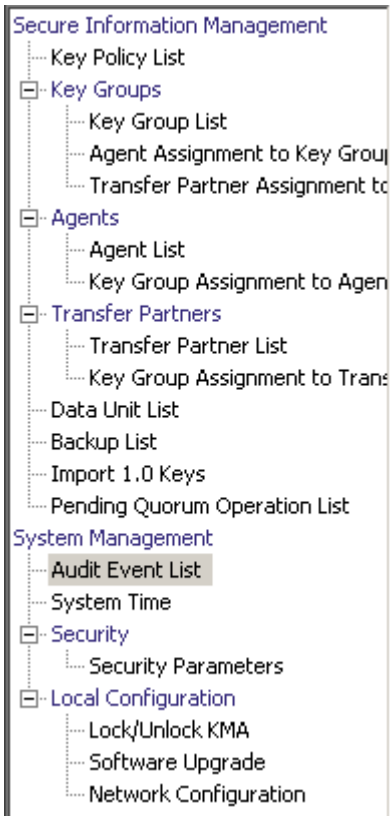
このボタンをクリックすると、ファイルの場所を指定できます。

起動

このボタンをクリックすると、KMS 1.0 の鍵ファイルの KMA へのアップロードが開始されます。ファイルに含まれる鍵ごとに、新しい鍵が作成されます。新しい鍵はそれぞれ、選択した鍵グループに関連付けられます。ファイルがアップロードされ適用された時間を示すメッセージが表示されます。

「Audit Event List」メニュー

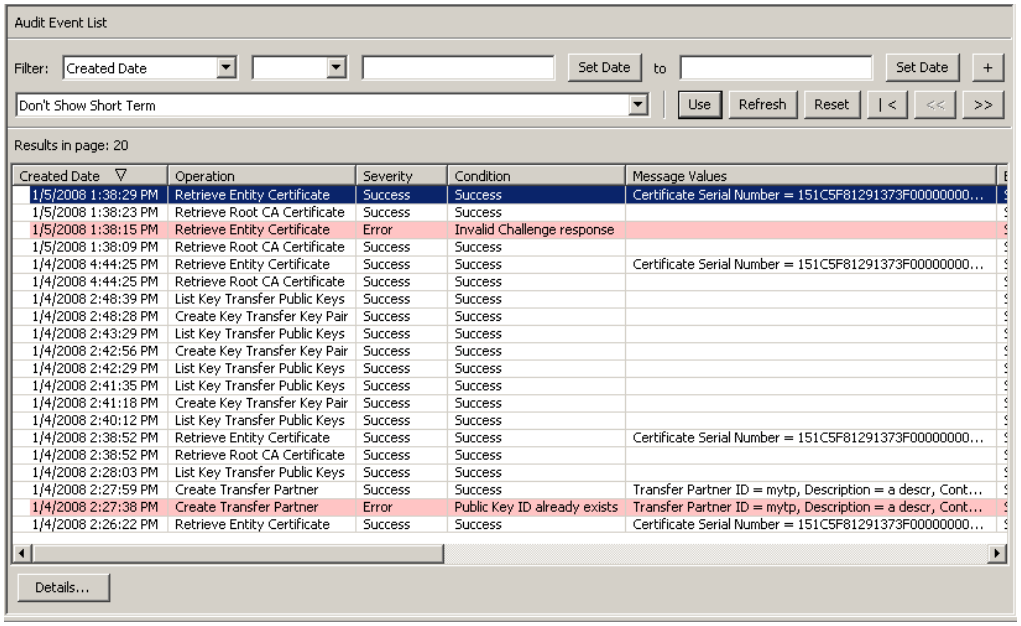
「Audit Event List」メニューを使用すると、監査ログイベントを表示できます。



監査ログの表示

監査ログイベントを表示するには、次の手順を実行します。

「System Management」メニューから「**Audit Event List**」を選択します。「Audit Event List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーで監査イベントリストにフィルタを適用することもできます。

- 作成日
- 操作
- 重要度
- 条件
- Entity ID
- Entity Network Address
- KMA ID
- KMA 名
- Class
- Retention Term
- Audit Log ID

表示されている監査ログのリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- 作成日
- 操作
- 重要度
- 条件
- Entity ID
- Entity Network Address
- KMA 名
- Class
- Retention Term
- Audit Log ID

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 空白
- 空白以外

フィルタ値 1 ボックス :

日付フィルタを選択した場合は、「**Set Date**」をクリックして開始日付と開始時刻を指定します。値は、フィルタキーの範囲の開始値として表示されます。ほかのフィルタを選択した場合は、このフィールドに値を入力します。

フィルタ値 2 ボックス :

日付フィルタを選択した場合は、「**Set Date**」をクリックして終了日付と終了時刻を選択します。値は、フィルタキーの範囲の終了値として表示されます。

フィルタ値 3 ボックス :

下矢印ボタンをクリックし、次のいずれかのフィルタを選択します。

- Don't Show Short Term
- Show All Retentions

作成日

監査イベントが作成された日時が表示されます。

操作

監査イベントレコードが作成される原因となった操作が表示されます。

重要度

操作が失敗した場合の状況の重大度が示されます。「Success」(エラーなし)、「Warning」、または「Error」の値を取ります。

条件

操作が正常に完了したかどうかが示されます。

> **注 ー** エラーは赤色で強調表示され、警告は黄色で強調表示されます。エラーメッセージの上にカーソルを置くと、エラーの詳細な説明が表示されます。

Event Message

監査イベントエントリの詳細情報が表示されます。

Entity ID

この監査イベントがユーザー、エージェント、またはピア KMA から要求された操作に応答して生成されている場合、このフィールドには、その実体のユーザー指定の識別子が表示されます。それ以外の場合、このフィールドは空白です。

Entity Network Address

この監査イベントがユーザー、エージェント、またはピア KMA から要求された操作に応答して生成されている場合、このフィールドには、その実体のネットワークアドレスが表示されます。それ以外の場合、このフィールドは空白です。

KMA ID

この監査イベントを生成した KMA の名前を表示します。この KMA 名は、クラスタ内の各 KMA を区別するためのユーザーが指定した識別子です。

KMA Name

クラスタ内の各アプライアンスを識別するユーザー指定の識別子が表示されます。

Class

監査イベントエントリが属する操作のクラスが示されます。取り得る値は次のとおりです。

- Agent Access Control Management Operations
- Agent Client Generated Audits
- Agent Management Operations
- Appliance Management Operations
- Audit Log Agent Operations
- Audit Log Management Operations
- Audit Log Operations
- Backup Management Operations
- CA Operations
- Cluster Client Communication
- Cluster Operations

- Communication and Authentication
- Console Security Management Operations
- Data Unit Agent Operations
- Data Unit Management Operations
- Discovery Operations
- Key Group Agent Operations
- Key Group Management Operations
- Key Policy Management Operations
- License Key Management Operations
- Local Management Operations
- Management Client Generated Audits
- Passphrase Agent Operations
- Replication Operations
- Retrieve Certificate Operations
- Role Management Operations
- SNMP Management Operations
- Security Management Operations
- Security Parameter Management Operations
- Security Violation
- Site Management Operations
- System Messages
- User Management Operations

Retention Term

監査イベントレコードの定義された保持期間が表示されます。取り得る値は、「Long Term」、「Medium Term」、および「Short Term」です。

Long Term

長い期間格納する必要のあるイベントレコード。

Medium Term

中程度の期間格納する必要のあるイベントレコード。

Short Term

短い期間格納する必要のあるイベントレコード。

Audit Log Entry ID

監査イベントエントリの各タイプを識別する一意のシステム生成識別子が表示されます。

Audit Log ID

各監査イベントエントリを識別する一意のシステム生成識別子が表示されます。

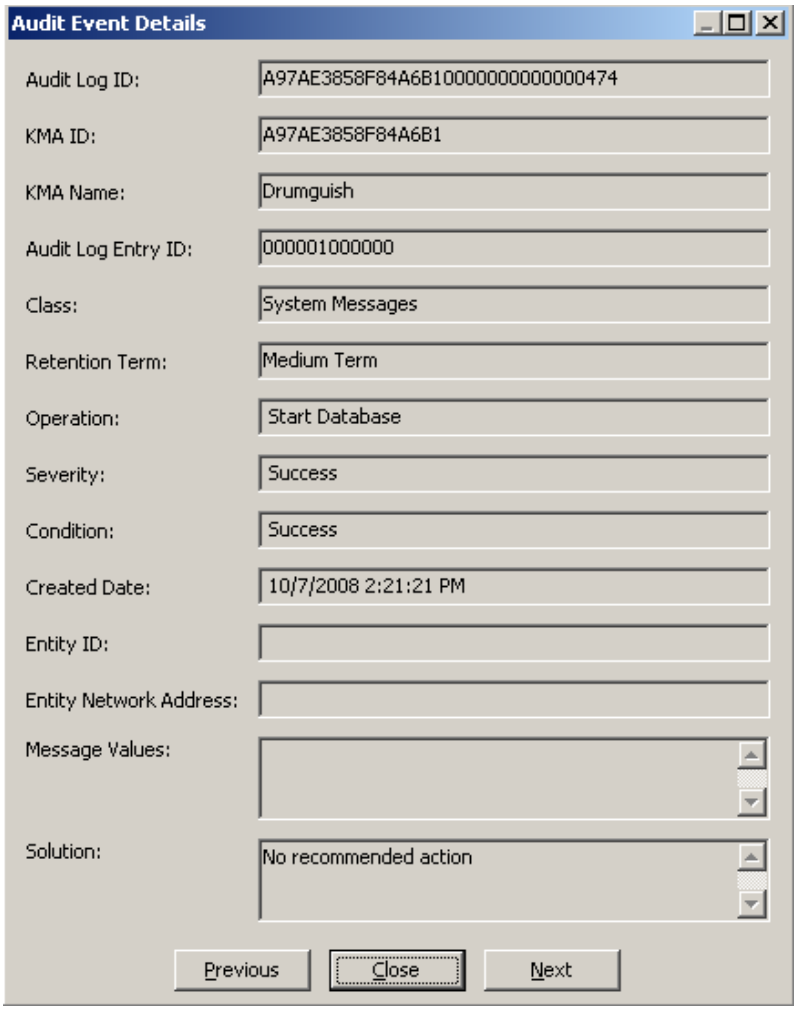
監査ログに関する詳細情報を表示する場合は、その監査ログを強調表示して「**Details**」ボタンをクリックします。詳細は、「監査ログの詳細の表示」を参照してください。

監査ログをエクスポートするには、「**Export**」ボタンをクリックします。詳細については、288 ページの「監査ログのエクスポート」を参照してください。

監査ログの詳細の表示

監査ログの詳細を表示するには、次の手順を実行します。

1. 「Audit Event List」画面から、詳細情報を表示する監査ログエントリを選択して「**Details**」ボタンをクリックするか、またはそのエントリをダブルクリックします。「Audit Event Details」ダイアログボックスが表示されます。このダイアログボックスでは、「**Previous**」、「**Close**」、および「**Next**」ボタンを除くすべてのフィールドが無効になっています。



2. 前または次の監査イベントにアクセスするには、「**Previous**」または「**Next**」ボタンをクリックします。「Audit Event List」画面に戻るには、「**Close**」ボタンをクリックします。

監査ログのエクスポート

エクスポート機能を使用すると、すべてまたは特定の監査ログエントリをワークステーション上のテキストファイルにエクスポートできます。次に、そのファイルをスプレッドシートアプリケーションで表示できます。

監査ログをエクスポートするには、次の手順を実行します。

1. 「Audit Event List」画面で、「View」メニューから「**`Save Report...`**」を選択するか、または Ctrl-S を押します。
2. 完了したら、「**Start**」ボタンをクリックしてエクスポートプロセスを開始します。「Audit Event List」画面でエントリにフィルタを適用した場合は、該当するエントリのみがエクスポートされます。フィルタを適用していない場合は、すべての監査イベントがエクスポートされます。
3. エクスポート処理が完了すると、エクスポートされた監査ログの数が、ダイアログボックスの下部に表示されます。
4. このダイアログボックスを閉じて「Audit Event List」画面に戻るには、「**Close**」ボタンをクリックします。

「Data Unit List」メニュー

「Data Unit List」メニューを使用すると、次を行うことができます。

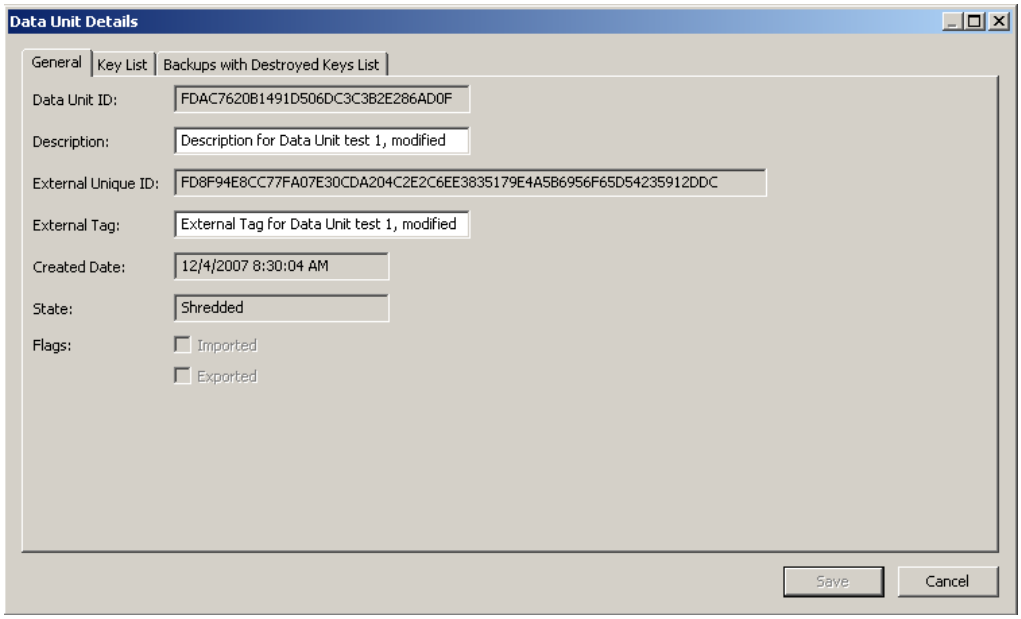
- データユニットの表示
- データユニットの詳細の表示および変更
- データユニットの活動履歴の表示
- データユニットの運用後鍵の破棄

「Data Units」メニューの使用法については、309 ページの「「Data Unit List」メニュー」を参照してください。

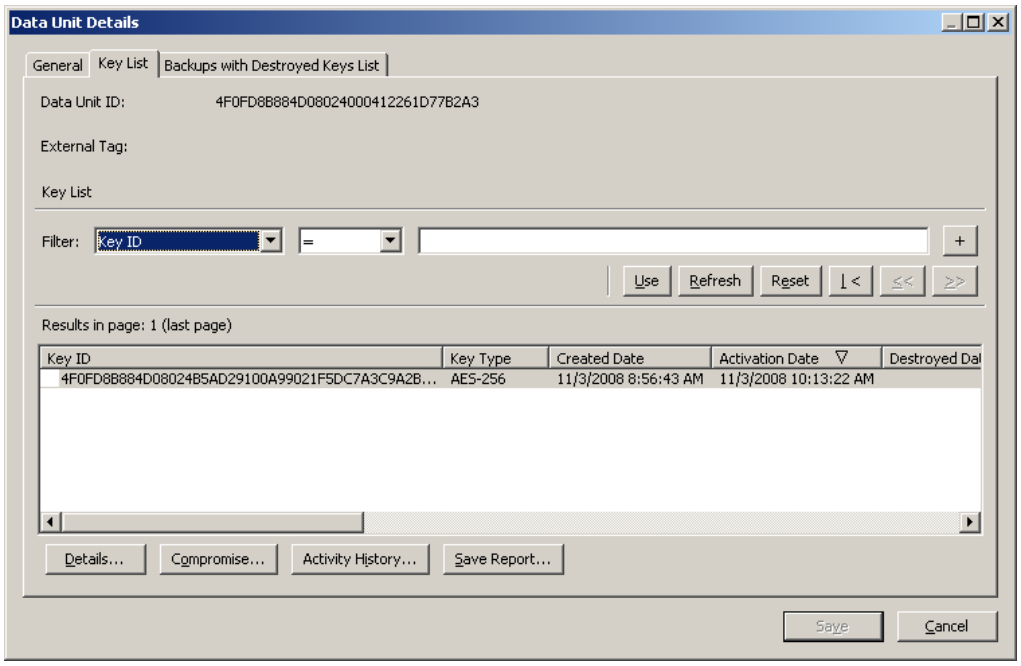
鍵の危殆化

コンプライアンス責任者は、鍵を危殆化することを承認されています。

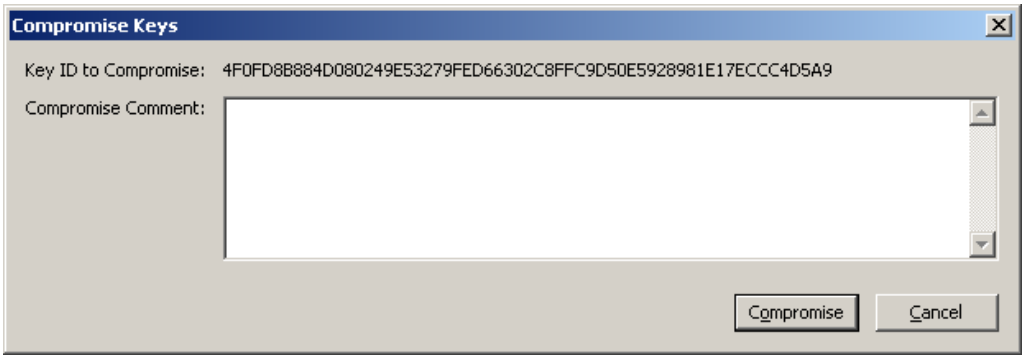
1. 「Data Unit List」画面から、変更するデータユニットを選択して「**Details**」ボタンをクリックします。「Data Unit Details」ダイアログボックスが表示されます。



2. 「Key List」タブをクリックして、このデータユニットに関連付けられた鍵を表示します。



3. 危殆化する鍵を選択し、「**Compromise**」ボタンをクリックします。鍵の危殆化を確認するダイアログボックスが表示されます。
4. 「**Yes**」ボタンをクリックします。次のダイアログボックスが表示され、コメントを入力するよう求められます。



5. 選択された鍵の危殆化に関するコメントを入力します。「**Compromise**」ボタンをクリックした場合は、鍵の危殆化を確認する別のダイアログボックスが表示されます。
6. 「**Yes**」ボタンをクリックします。危殆化された鍵の数を示すダイアログボックスが表示されます。

その他の機能

コンプライアンス責任者は、次の操作を行うこともできます。

- 監査イベントリストの表示
- システム時刻の表示
- KMA 状態のロックおよびロック解除

これらの機能の手順については、第 5 章「セキュリティー責任者の操作」を参照してください。

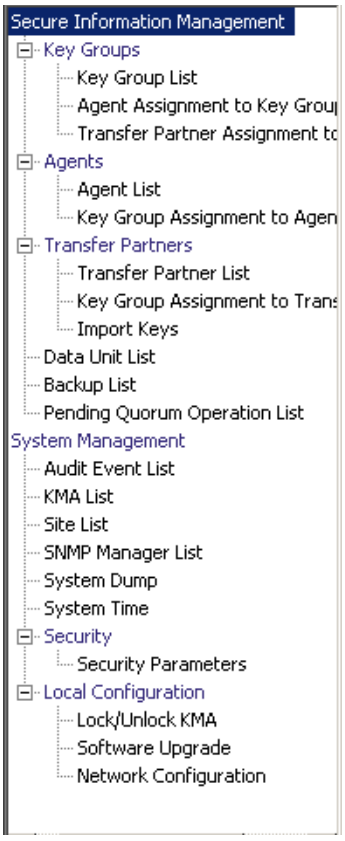
7

オペレータの操作

この章では、オペレータの役割が付与されたユーザーが実行できる操作について説明します。複数の役割が割り当てられている場合は、その役割を実行する手順について、該当する章を参照してください。

オペレータの役割

オペレータは、システムの日常業務を管理します。



「Key Groups」メニュー

「Key Groups」メニューを使用すると、次を行うことができます。

- 鍵グループのリストの表示
- 鍵グループへのエージェントの割り当ての表示
- 鍵グループへの転送パートナーの割り当ての表示

Key Group List

「Key Group List」メニューオプションを使用すると、鍵グループを管理できます。手順については、252 ページの「「Key Group List」メニュー」を参照してください。

Agent Assignment to Key Groups

「Agent Assignment to Key Groups」メニューオプションを使用すると、鍵グループに割り当てられているエージェントを表示できます。手順については、260 ページの「「Agent Assignment to Key Groups」メニュー」を参照してください。

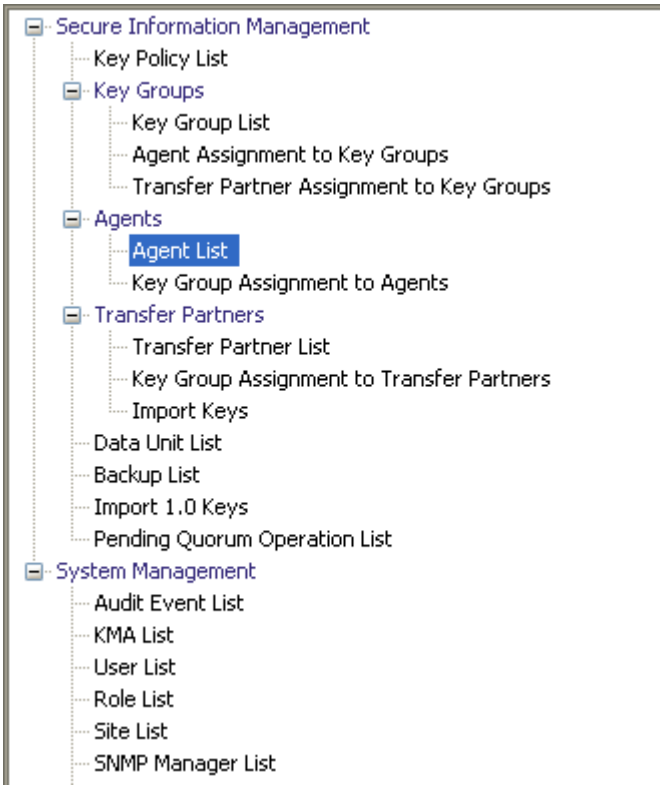
Transfer Partner Assignment to Key Groups

「Transfer Partner Assignment to Key Groups」オプションを使用すると、特定の鍵グループへのアクセスを許可されている一連の鍵転送パートナーの 1 つを表示できます。手順については、276 ページの「「Transfer Partner Assignment to Key Groups」メニュー」を参照してください。

「Agent List」メニュー

「Agent List」メニューオプションを使用すると、次の操作を行うことができます。

- エージェントの表示
- エージェントの作成
- エージェントの表示および変更
- 既存のエージェントの削除

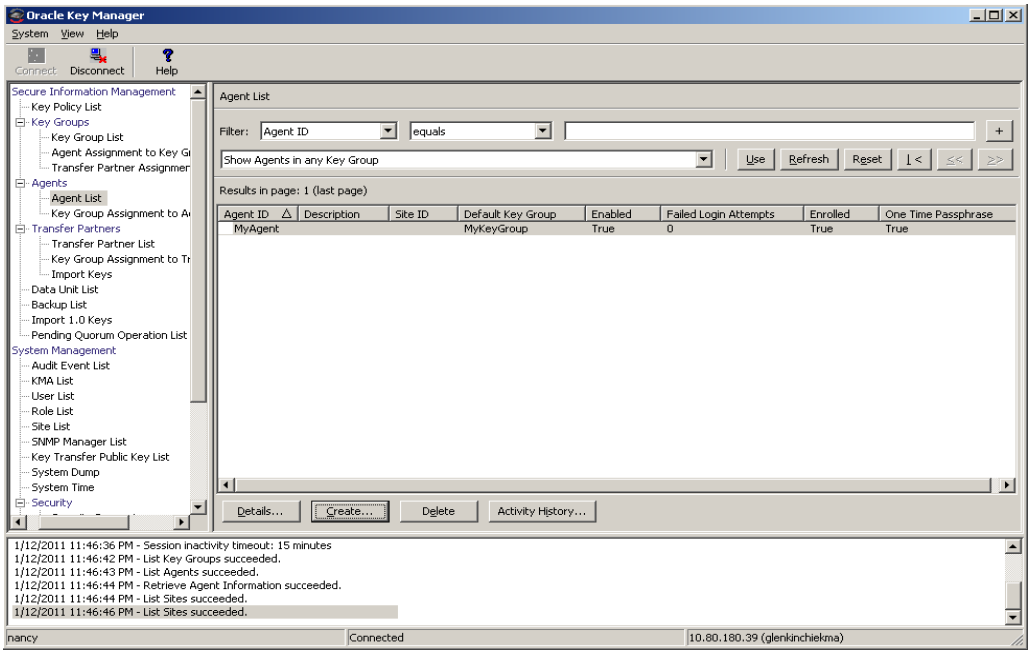


エージェントリストの表示

「Agent List」メニューオプションを使用すると、特定の鍵グループに関連付けられているすべてのエージェントを表示できます。

この画面を表示するには、次の手順を実行します。

1. 「Agents」メニューから、「**Agent List**」を選択します。「Agent List」画面が表示されます。
2. 鍵グループのフィールドの横にある下矢印ボタンをクリックし、鍵グループを選択します。鍵グループに関連付けられているエージェントが表示されます。



リスト全体をスクロールするか、次のいずれかのキーでエージェントにフィルタを適用することもできます。

- エージェント ID
- 説明
- サイト
- Default Key Group
- 有効
- Failed Login Attempts
- Enrolled
- One Time Passphrase

表示されているエージェントリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ：

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- エージェント ID
- 説明
- サイト
- Default Key Group
- 有効
- Failed Login Attempts
- Enrolled

フィルタ演算子ボックス：

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス：

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス：

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用：

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

エージェント ID

各エージェントを識別するユーザー指定の一意の識別子が表示されます。

説明

エージェントの説明が示されます。

サイト

エージェントが属しているサイトを示す一意の識別子が表示されます。

Default Key Group

エージェントで別の鍵グループが明示的に指定されていない場合、このエージェントによって作成されるすべての鍵に関連付けられる鍵グループ。

有効

エージェントの状態を示します。True または False の値を取ります。このフィールドが False の場合、エージェントは KMA とのセッションを確立できません。

Failed Login Attempts

ログオンに失敗した回数が表示されます。

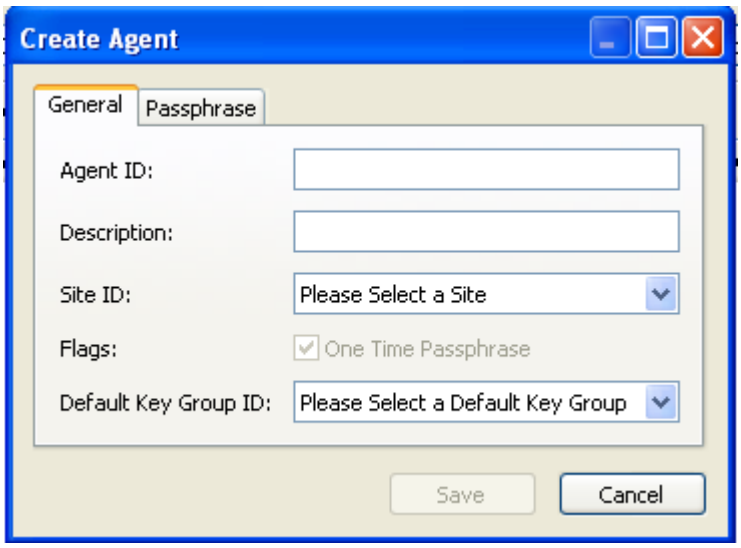
Enrolled

エージェントが OKM クラスタに正常に登録されたかどうかを示します。True または False の値を取ります。エージェントがはじめて作成されたか、またはエージェントのパスフレーズが変更された場合、このフィールドは False になります。

エージェントの作成

エージェントを作成するには、次の手順を実行します。

1. 「Agent List」画面から、「**Create**」ボタンをクリックします。「Create Agent」ダイアログボックスが表示され、「General」タブが開きます。



2. 次のパラメータを設定します。

エージェント ID

エージェントを一意に識別する値を入力します。この値は、1 ～ 64 文字で指定できます。

説明

エージェントを説明する値を入力します。この値は、1 ～ 64 文字で指定できます。

Site ID

下矢印ボタンをクリックし、エージェントが属するサイトを強調表示します。このフィールドは省略可能です。

フラグ

エージェントがパスフレーズをリセットし、エージェント ID と新しいパスフレーズで再登録しなければ X.509 証明書を取得できないようにするには、「**One Time Passphrase**」を選択します。これはデフォルトです。

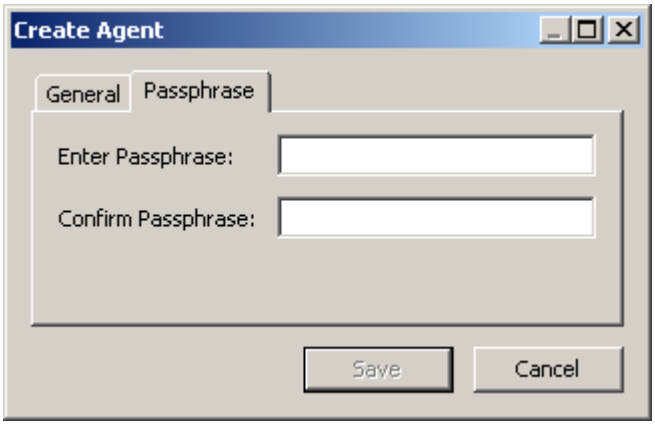
「**One Time Passphrase**」にチェックマークを付けない場合、エージェントはいつでも X.509 証明書を取得し、CA と証明書サービスを使用して、エージェント ID とパスフレーズによって正常に認証できます。

テープドライブエージェントは、デフォルト値を指定するようにしてください。PKCS#11 タイプのエージェントの場合、特にユーザーが複数のノードから OKM に対して認証される可能性のあるクラスタ構成では、この設定がより便利になります。

Default Key Group ID

下矢印ボタンをクリックし、デフォルトの鍵グループを強調表示します。

3. 「Passphrase」タブを開きます。



4. 次のパラメータを設定します。

パスフレーズ

このユーザーのパスフレーズを入力します。最小文字数は 8 文字、最大文字数は 64 文字です。デフォルト値は 8 です。

パスフレーズの要件は、次のとおりです。

- パスフレーズに、ユーザーのエージェント ID を含めないでください。
- パスフレーズには、大文字、小文字、数値、または特殊文字の 4 つの文字クラスのうち 3 つを使用する必要があります。

  使用可能な特殊文字は、次のとおりです。

  ‘ ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ’ ” < > , . / ?

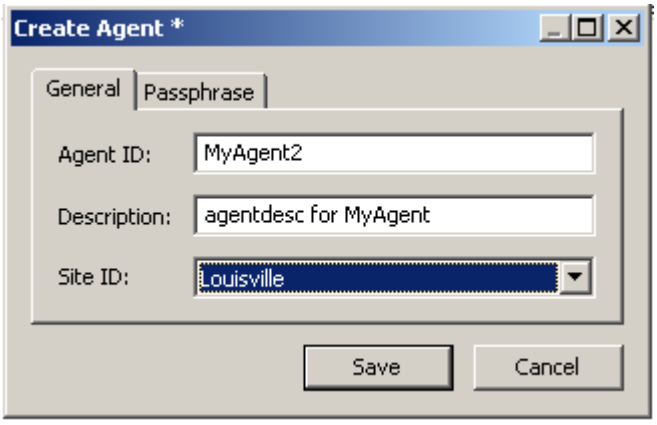
  n タブ、改行などの制御文字は使用できません。

  注 ー パスフレーズの最小文字数の要件を変更する方法については、211 ページの「セキュリティーパラメータの変更」を参照してください。

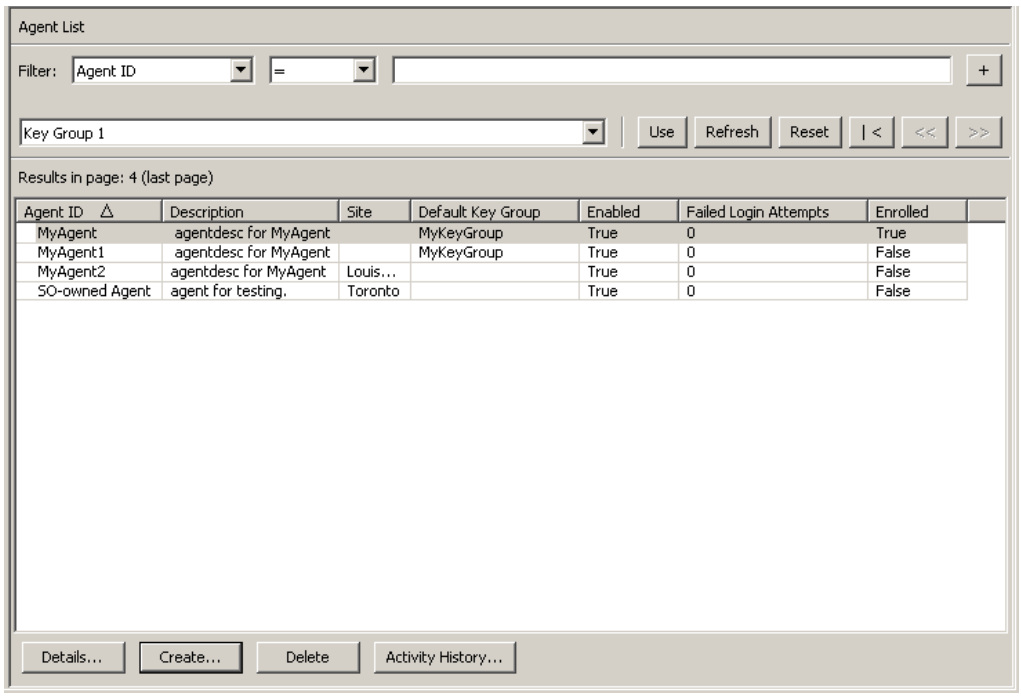
Confirm Passphrase

「Enter Passphrase」フィールドに入力した値と同じ値を入力します。

値を入力した「Create Agent」ダイアログボックスの例を次に示します。



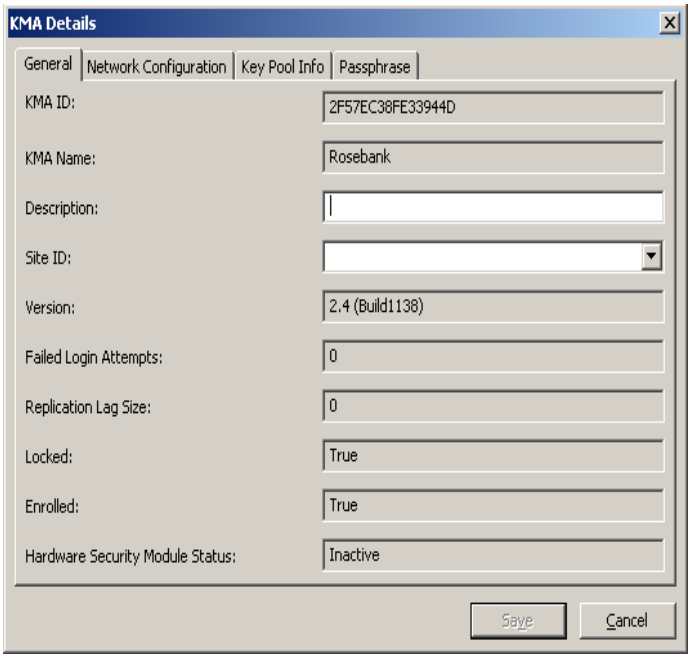
5. 「**Save**」ボタンをクリックします。エージェントレコードがデータベースに追加され、「Agent List」画面に表示されます。
6. エージェント固有のインタフェースを使用して、エージェント固有の登録手順を完了します。たとえば、StorageTek ドライブの場合は、VOP (Virtual Operator Panel) を使用して登録手順を完了する必要があります。



エージェントの表示および変更

エージェントの詳細を変更するには、次の手順を実行します。

1. 「Agent List」画面から、詳細情報を表示するエージェントエントリをダブルクリックするか、またはそのエージェントエントリを強調表示して「**Details**」ボタンをクリックします。「Agents Details」ダイアログボックスが表示されます。



2. 「General」タブを開き、必要に応じて次のフィールドを変更します。

- 説明
- Site ID

- フラグ
  - 「Enabled」- このエージェントがクラスタと通信できるようにする場合は、このチェックボックスを選択します。
  - 「Enrolled」- エージェントがクラスタに正常に登録されたかどうかを示します。このフィールドは読み取り専用です。
  - 「One Time Passphrase」- エージェントがパスフレーズをリセットし、エージェント ID と新しいパスフレーズで再登録しなければ X.509 証明書を取得できないようにするには、このチェックボックスを選択します。これはデフォルトです。

    「**One Time Passphrase**」にチェックマークを付けない場合、エージェントはいつでも X.509 証明書を取得し、CA と証明書サービスを使用して、エージェント ID とパスフレーズによって正常に認証できます。

    テープドライブエージェントは、デフォルト値を指定するようにしてください。PKCS#11 タイプのエージェントの場合、特にユーザーが複数のノードから OKM に対して認証される可能性のあるクラスタ構成では、この設定がより便利になります。
- 「Default Key Group ID」-下矢印ボタンをクリックし、デフォルトの鍵グループを強調表示します。

3. 終了したら、「**Save**」ボタンをクリックします。OKM Manager データベースに対して変更が加えられ、「Agent List」画面に戻ります。

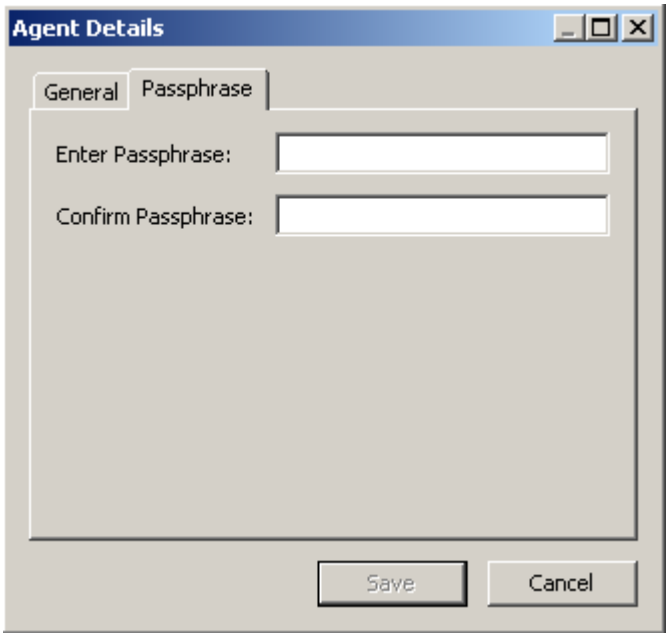
   注 ー
   エージェントのパスフレーズは、そのパスフレーズが危殆化されたと考えられる場合にのみ変更するようにしてください。手順については、304 ページの「エージェントのパスフレーズの設定」を参照してください。

エージェントのパスフレーズの設定

エージェントのパスフレーズを設定すると、エージェントが KMA で認証を受けるためのエージェント証明書を失効させることができます。エージェント証明書またはパスフレーズ、あるいはその両方が危殆化されていると思われる場合、オペレータは、エージェントのパスフレーズ証明書を設定できます。

エージェントのパスフレーズを設定するには、次の手順を実行します。

1. 「Agent List」画面から、パスフレーズを設定するエージェントエントリをダブルクリックするか、またはそのエージェントエントリを強調表示して「**Details**」ボタンをクリックします。「Agent Details」ダイアログボックスが表示されます。「Passphrase」タブを開きます。



2. 次のフィールドを変更し、「Save」ボタンをクリックします。

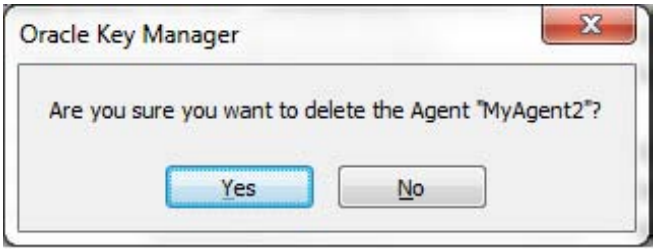
- Enter Passphrase
- Confirm Passphrase

3. データベースが変更され、「Agents List」画面に戻ります。
4. エージェント固有の手順で、エージェントを再登録します。たとえば、StorageTek テープドライブの場合は、VOP (Virtual Operator Panel) を使用してエージェントを OKM クラスタに再登録する必要があります。エージェントのパスフレーズを変更すると、そのエージェントは、再登録されるまで OKM クラスタに要求を送信できなくります。

エージェントの削除

エージェントを削除するには、次の手順を実行します。

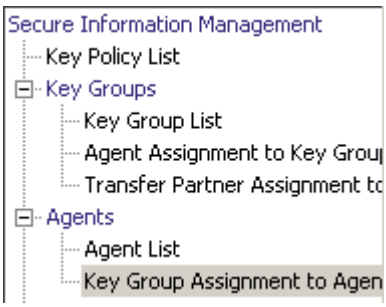
1. 「Agents List」画面で、削除するエージェントを強調表示します。次のように、選択したエージェントの削除を確認するダイアログボックスが表示されます。



2. 「**Yes**」ボタンをクリックして、エージェントを削除します。エージェントがデータベースから削除され、「Agents List」画面に戻ります。削除したエージェントは表示されなくなります。

「Key Group Assignment to Agents」メニュー

「Key Group Assignment to Agents」メニューオプションを使用すると、エージェントに割り当てられている鍵グループを表示できます。手順については、266 ページの「「Key Group Assignment to Agents」メニュー」を参照してください。



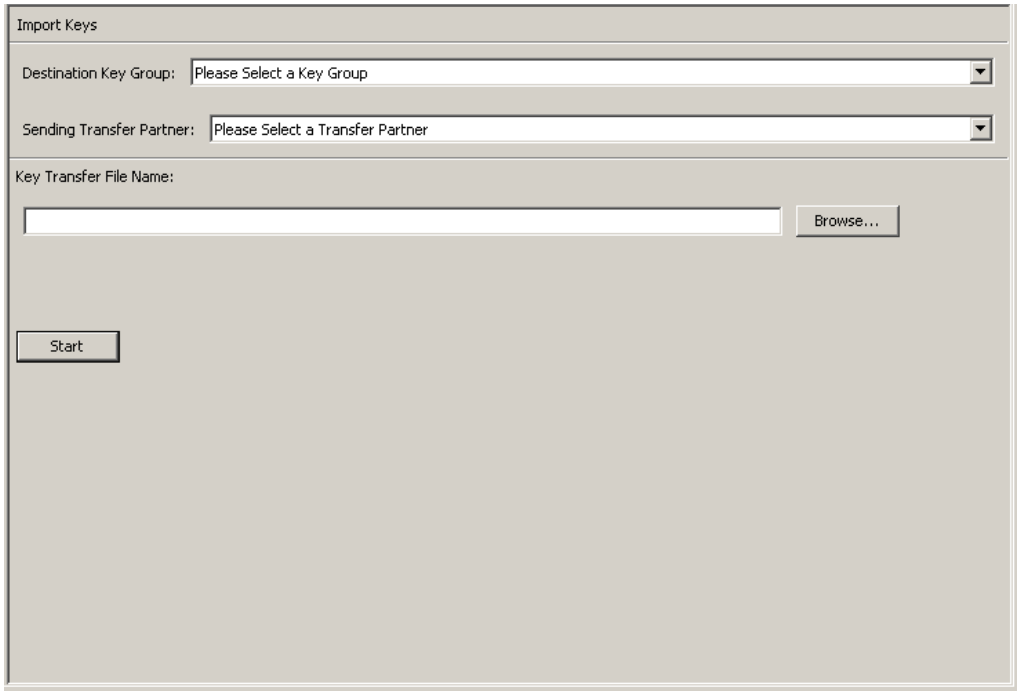
「Import Keys」メニュー

このメニューオプションは、鍵とデータユニットを OKM クラスタにインポートします。鍵とデータユニットの情報は、鍵転送パートナーから受信された鍵転送ファイルに含まれています。

> **注 ー** この画面は、鍵を OKM クラスタにアップロードしてインポートするために使用します。これらの鍵は、別の OKM クラスタからエクスポートされます。

鍵をインポートするには、次の手順を実行します。

1. 「Transfer Partners」メニューから「**Import Keys**」を選択します。「Import Keys」画面が表示されます。



2. 次のパラメータを設定します。

Destination Key Group:

これらの鍵のインポート先となる鍵グループを選択します。

この鍵グループの鍵ポリシーの「Allow Imports」フラグがオンになっている必要があります。この鍵グループは、選択した送信側転送パートナーに対して許可された鍵グループである必要があります。

Sending Transfer Partner:

これらの鍵をエクスポートした送信側転送パートナーを選択します。

Key Transfer File:

鍵転送ファイルの名前を入力します。また、「**Browse**」をクリックして宛先パスを選択することもできます。

3. 「**Start**」ボタンをクリックして、アップロードおよび鍵インポートプロセスを開始します。ファイルがアップロードされて適用されたことを示すメッセージが表示されます。

データユニット

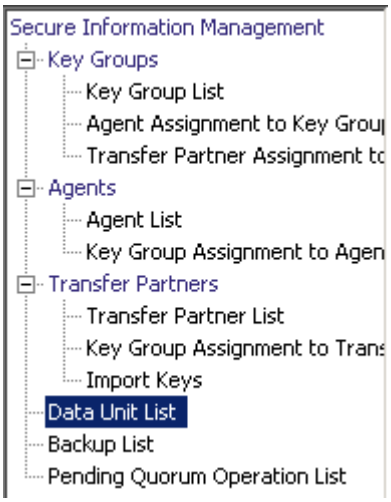
データユニットは、ディスク、テープ、オブジェクトなどの論理ストレージデバイスです。データユニットは、鍵グループに関連付けられている有効な鍵ポリシーによってセキュリティー保護されます。エージェントは、選択したデータユニットにアクセス可能である必要があります。

> **注 –** オペレータは、データユニットの鍵グループの変更を除くすべての機能を実行できます。データユニットの鍵グループを変更できるのは、コンプライアンス責任者のみです。

「Data Unit List」メニュー

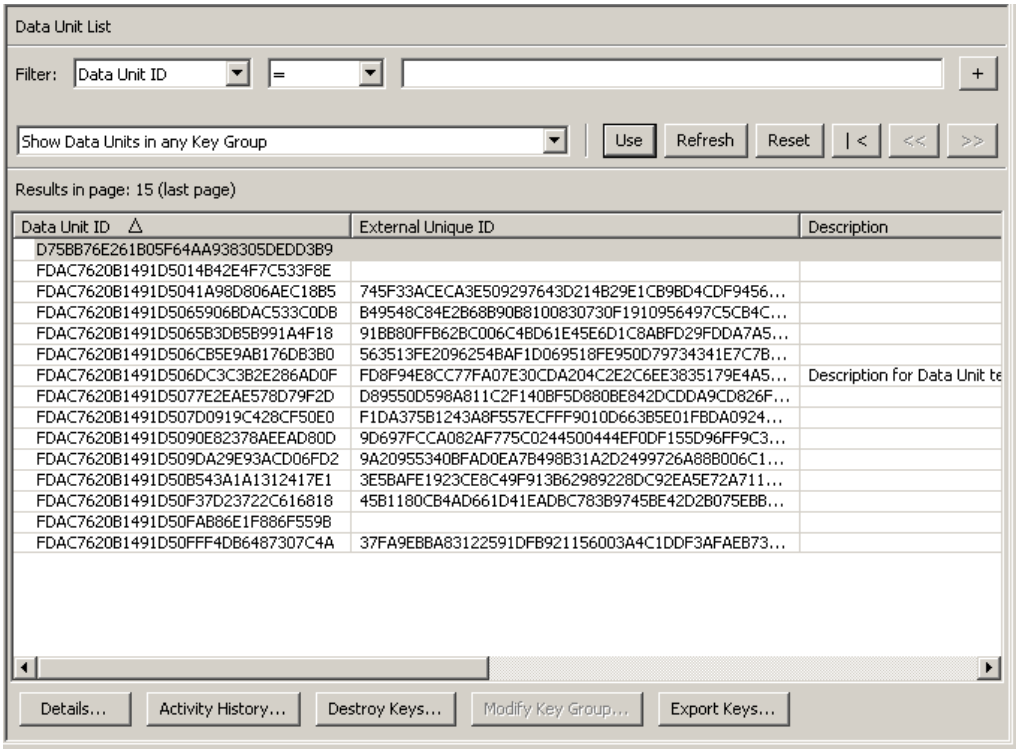
「Data Unit List」メニューを使用すると、次を行うことができます。

- データユニットの表示
- データユニットの詳細の表示および変更
- データユニットの活動履歴の表示
- データユニットの運用後鍵の破棄



データユニットの表示

データユニットを表示するには、「Data Units」メニューから「Data Unit List」を選択します。「Data Unit List」画面が表示されます。



データベース全体をスクロールするか、次のいずれかのキーでデータユニットリストにフィルタを適用することもできます。

- データユニット ID
- External Unique ID
- 説明
- External Tag
- 作成日
- Exported
- Imported
- 状態。

表示されているデータユニットリストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- データユニット ID
- External Unique ID
- 説明
- External Tag
- 作成日
- Imported
- Exported
- 状態 .

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

Show Data Units in Any Key Group. 使用 :

このボタンをクリックすると、表示されているリストにフィルタが適用されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

データユニット ID

各データユニットを識別する一意のシステム生成識別子が表示されます。

External Unique ID

データユニットの一意の外部識別子が表示されます。

この値はエージェントによって OKM に送信されるため、外部のエンドユーザーには表示されない可能性があります。LTO Gen 4 および Gen 5 テープの場合、この値は、製造時にカートリッジに焼き付けられたカートリッジのシリアル番号です。この値を、光学式バーコードや ANSI テープラベルのボリュームシリアル番号 (VOLSER) と混同しないでください。この値は、StorageTek テープドライブでは使用されません。

説明

データユニットの説明が示されます。

External Tag

データユニットの一意の外部タグの説明が示されます。

StorageTek テープライブラリ内に存在するテープ、または ANSI 標準ラベルの付いたテープの場合、このフィールドは volser になります。ライブラリ内に存在するテープに ANSI ラベルが付いているときに、ライブラリの volser (つまり、光学式バーコード) が ANSI ラベルに記載されている volser とは異なる場合は、ライブラリの volser が使用されます。ANSI ラベルを付けずにスタンドアロンドライブで書き込まれたテープの場合、このフィールドは空白になります。

注 ー LTO Gen 4 および Gen 5 テープドライブで書き込まれたデータユニットの場合は、32 文字を埋めるために、このフィールドの右側が空白でパディングされます。「External Tag」をパディングするために空白を追加しなくても済むように、「Equals =」フィルタ演算子の代わりに「Starts With ~」フィルタ演算子を使用した方が便利な場合があります。

たとえば、「Starts With」フィルタを使用する場合は、次のように入力できます。

"External Tag" ~ "ABCDEF"

同じ例で「Equals」フィルタを使用する場合は、次のように入力する必要があります。

"External Tag" = "ABCDEF "
(32 文字を埋めるためにパディングされている)

作成日

データユニットが作成または登録された日時を示します。

Exported

このデータユニットに関連付けられている鍵がエクスポートされたかどうかを示します。

Imported

このデータユニットに関連付けられている鍵がインポートされたかどうかを示します。

説明

データユニットの状態を示します。取り得る値は次のとおりです。

- **「No Key」:** データユニットが作成されたが、まだ鍵が作成されていない場合に設定されます。
- **「Readable」:** データユニットに、そのデータユニットの少なくとも一部を復号化できる (読み取ることのできる) 鍵が存在する場合に設定されます。
- **「Normal」:** データユニットに、そのデータユニットの少なくとも一部を復号化できる (読み取ることのできる) 鍵が存在する場合に設定されます。さらに、データの暗号化に使用できる「Protect-and-Process」状態の鍵が、データユニット内に 1 つ以上存在します。したがって、データユニットは書き込み可能になります。
- **「Needs ReKey」:** データユニットに、そのデータユニットの少なくとも一部を復号化できる (読み取ることのできる) 鍵が存在する場合に設定されます。ただし、「Protect-and-Process」状態の鍵は、データユニット内に 1 つもありません。

  データがこのテープに書き込まれると、新しい「Protect-and-Process」状態の鍵がデータユニットに自動的に付与されます。
- **「Shredded」:** このデータユニットのすべての鍵が破棄された場合に設定されます。データユニットの読み取りまたは書き込みを行うことはできません。ただし、このデータユニットに対して新しい鍵を作成することができ、作成するとデータユニットの状態は「Normal」に戻ります。

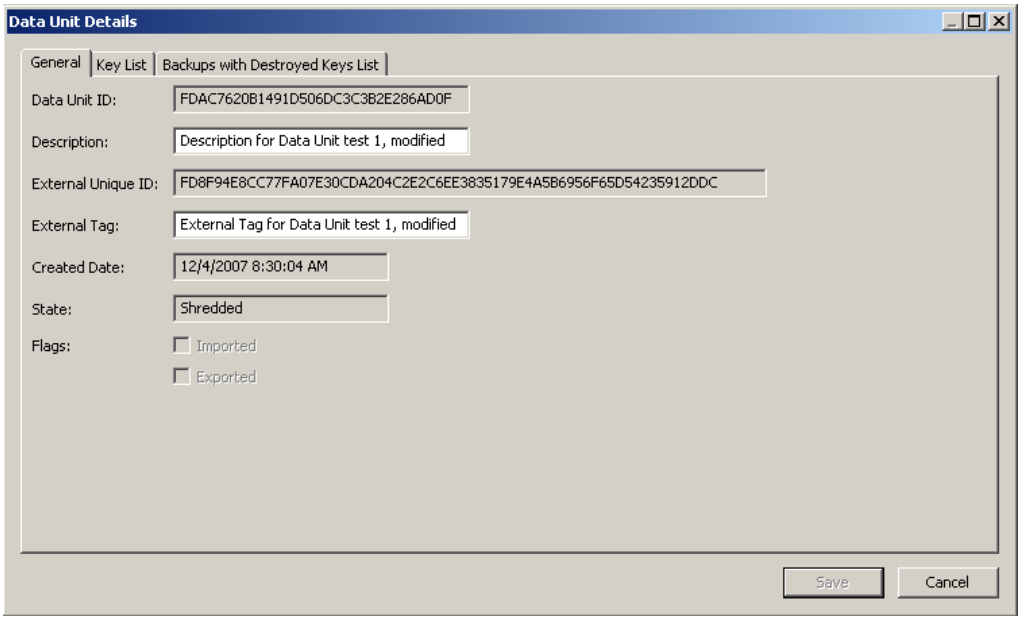
データユニットの詳細の表示および変更

注 ー ユーザーがオペレータでない場合は、データユニットの詳細情報を表示すると、すべてのフィールド (「**Save**」ボタンを含む) が無効になります。ユーザーがコンプライアンス責任者である場合は、「Key Group」フィールドが有効になります。

「Key List」タブにある「**Compromise**」ボタンは、ユーザーがコンプライアンス責任者である場合は有効、それ以外の場合は無効になります。

データユニットの情報を変更するには、次の手順を実行します。

1. 「Data Unit List」画面から、変更するデータユニットを選択して「**Details**」ボタンをクリックします。「Data Unit Details」ダイアログボックスが表示されます。



2. 次のパラメータを変更できます。

説明

新しい値を入力します。元の情報は、登録時にソフトウェア暗号化ドライバによって提供されたものです。この値は 1 ～ 64 文字、または空白で指定できます。

重要 ー 「Description」フィールドに「`PKCS#11v2.20`」の文字列が含まれている場合は、Oracle Database の透過的データ暗号化 (TDE) に使用される特殊鍵を表します。このフィールドを変更しないでください。変更すると、OKM での TDE の処理方法が変更される場合があります。

External Tag

データユニットの一意の外部識別子を入力します。この値は 1 ～ 64 文字、または空白で指定できます。このフィールドには、通常、テープカートリッジのラベルまたはバーコードが表示されます。

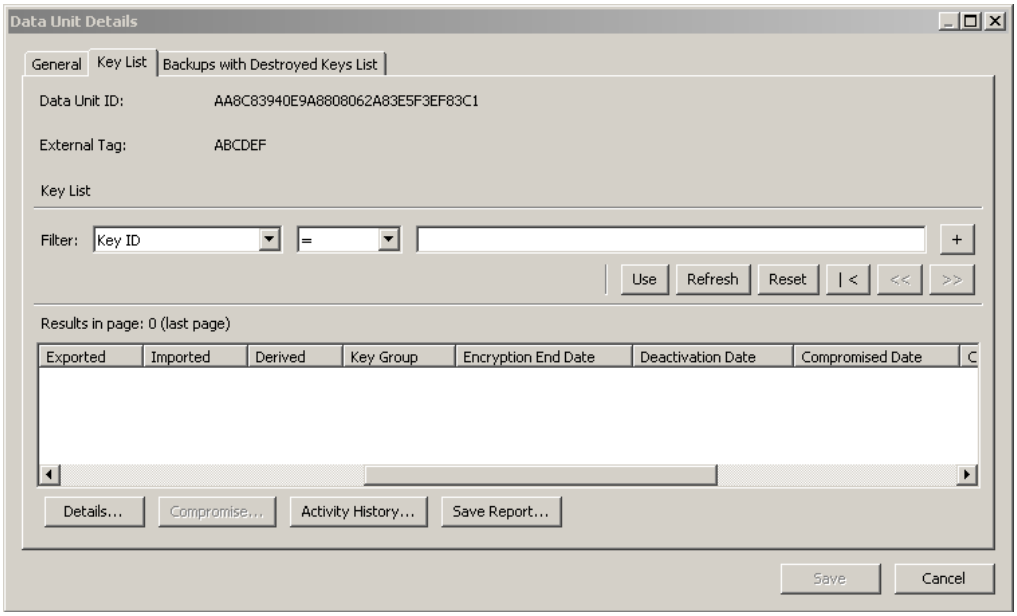
3. 「**Save**」ボタンをクリックして変更を保存します。

次のフィールドは編集できません。

「General」タブ

- データユニット ID
- External Unique ID
- 作成日
- 説明
- Flags Imported/Exported

「Key List」タブ



データユニット ID

データユニットを一意に識別します。

Data Unit Description

データユニットの説明が示されます。

Key ID

データユニットの鍵情報が表示されます。

Key Type

この鍵が使用する暗号化アルゴリズムのタイプを示します。取り得る値は AES-256 だけです。

作成日

鍵が作成された日時が表示されます。

Activation Date

鍵が有効になった日時が表示されます。これは、鍵が最初にエージェントに付与された日時です。また、鍵の暗号化期間と暗号化有効期間が開始する日付と時刻でもあります。

Destroyed Date

鍵が破棄された日付が表示されます。このフィールドが空白である場合、鍵は破棄されていません。

Destruction Comment

鍵の破棄に関するユーザーが指定した情報が表示されます。このフィールドが空白である場合、鍵は破棄されていません。

Exported

データユニットがエクスポートされたかどうかが示されます。

Imported

データユニットがインポートされたかどうかが示されます。

派生した

その鍵が、マスター鍵プロバイダによって生成されたマスター鍵から派生したかどうかを示します。詳細については、『OKM-ICSF Integration Guide』を参照してください。

Key Group

データユニットに関連付けられた鍵グループが表示されます。

Encryption End Date

鍵が使用されなくなった日時、またはデータの暗号化に使用されなくなった日時が表示されます。

Deactivation Date

鍵が無効になる日時、または無効になった日時が表示されます。

Compromised Date

鍵が危殆化された日付が表示されます。このフィールドが空白である場合、鍵は危殆化されていません。

Compromised Comment

鍵の危殆化に関するユーザーが指定した情報が表示されます。このフィールドが空白である場合、鍵は危殆化されていません。

Key State

データユニットの鍵の状態を示します。取り得る値は次のとおりです。

Generated

鍵が OKM クラスタ内のいずれかの KMA 上で作成された場合に設定されます。この状態の鍵は、マルチ OKM クラスタ内のほかの少なくとも 1 つの KMA に複製されるまで、生成済みのままになります。単一の KMA のみで構成されるクラスタでは、少なくとも 1 つのバックアップに記録されるまで、鍵は「Generated」状態のままになります。

準備完了

複製またはバックアップによって鍵が損失しないように保護されている場合は、この値に設定されます。「Ready」状態の鍵は、割り当てに使用できます。

Protect and Process

暗号化エージェントが新しい鍵の作成を要求したときに、鍵がすでに割り当てられていると、この値に設定されます。この状態の鍵は、暗号化と復号化の両方に使用できます。

Process Only

鍵が割り当てられているが、鍵の暗号化期間を過ぎている場合には、この値に設定されます。この状態の鍵は、復号化には使用できますが、暗号化には使用できません。

Deactivated

鍵の暗号有効期間が過ぎているが、情報を処理 (復号化) するために鍵が必要となる可能性がある場合には、この値に設定されます。

Compromised

承認されていない実体に鍵が渡された場合、または承認されていない実体によって鍵が検出された場合には、この値に設定されます。この状態の鍵は、復号化には使用できますが、暗号化には使用できません。

Incompletely Destroyed

鍵が破棄されたが、1 つ以上のバックアップ内にまだ存在している場合には、この値に設定されます。

Completely Destroyed

破棄された鍵が存在していたすべてのバックアップが破棄された場合には、この値に設定されます。

Compromised and Incompletely Destroyed

危殆化された鍵が 1 つ以上のバックアップ内にまだ存在している場合には、この値に設定されます。

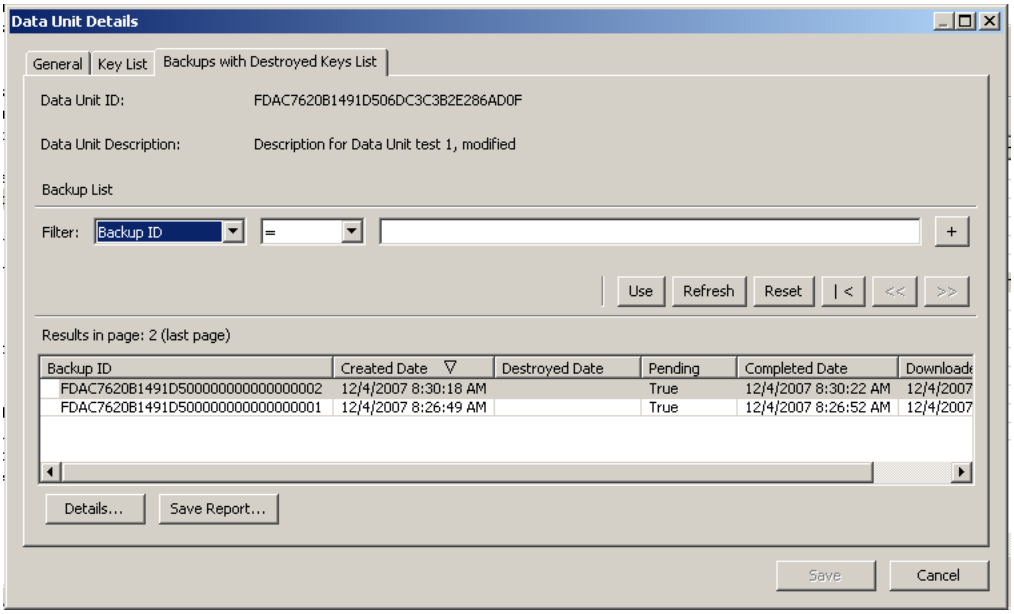
Compromised and Completely Destroyed

危殆化された鍵が存在していたすべてのバックアップが破棄された場合には、この値に設定されます。

Recovery Activated

回復操作によって鍵がデータユニットにリンクされたかどうかを示します。この状態は、鍵が OKM クラスタ内のいずれかの KMA によってデータユニットのために使用されたあと、障害のために、その鍵があとでそのデータユニットのために別の KMA から要求された場合に発生します。障害 (ネットワーク停止など) のために、データへの鍵の割り当てが 2 番目の KMA に伝播されなかった場合は、その 2 番目の KMA によってデータユニットへのリンクが作成されます。このような鍵は「Recovery Activated」状態になり、管理者が、システムで KMA またはネットワークの機能停止が発生しているかどうかを評価することになります。取り得る値は True と False です。

「Backups with Destroyed Keys List」タブ



データユニットは、データユニット鍵が含まれるすべてのバックアップが破棄されるまで、「Completely Destroyed」とは見なされません。

「Data Unit Details」ダイアログの「Backups with Destroyed Keys List」タブは、選択したデータユニットのデータユニット鍵が含まれるバックアップと、それらのバックアップの破棄の状態を特定するために役立ちます。

バックアップに特定のデータユニット鍵が含まれているかどうかは、次のように判断します。

バックアップにデータユニット鍵が含まれるのは、データユニット鍵が作成されたあとにバックアップが作成され、かつそのデータユニット鍵がまだ破棄されていない場合か、またはデータユニット鍵が破棄され、かつその破棄がバックアップが作成されたあとに実行された場合です。

ただし、日時を比較する場合は、クラスタ内のさまざまな KMA の時刻が自動的に同期化されていない (NTP サーバーが指定されていない) ため異なる時刻が報告される可能性を考慮する必要があります。KMA 間で時刻が違う可能性を考慮して、比較にはバックアップ時間枠が使用されます。バックアップ時間枠は、5 分間に固定されています。比較チェックは、バックアップ時間枠を使用して、次のように行われます。

バックアップにデータユニット鍵が含まれるのは、バックアップ作成以降の 5 分以内にバックアップが作成され、かつバックアップ作成以降の 5 分以内にデータユニット鍵が破棄された場合です。

バックアップ時間枠は、特定のバックアップ内のデータユニットが実際には存在しているのに、存在していないと誤って報告される可能性を最小限に抑えるために使用されます。このような状況は「偽陰性」と呼ばれ、これによりデータ破棄の適合性要件が非常に損なわれます。ただし、バックアップ時間枠を使用した場合には、バックアップ内のデータユニットが実際は存在していないのに、存在していると誤って報告される可能性が高くなります。「偽陰性」とは異なり、「偽陽性」はデータ破棄の適合性要件を損なうことがありません。

データユニット ID

データユニットを一意に識別します。

Data Unit Description

データユニットの説明が示されます。

Data Unit Destruction Status

データユニットの破棄の状態を示します。

Backup ID

バックアップを識別します。

作成日

バックアップファイルが作成された日時、つまりバックアップが開始された日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日時が表示されます。

保留中 :

バックアップがまだ保留中であることを示します。True または False の値を取ります。

Completed Date:

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date:

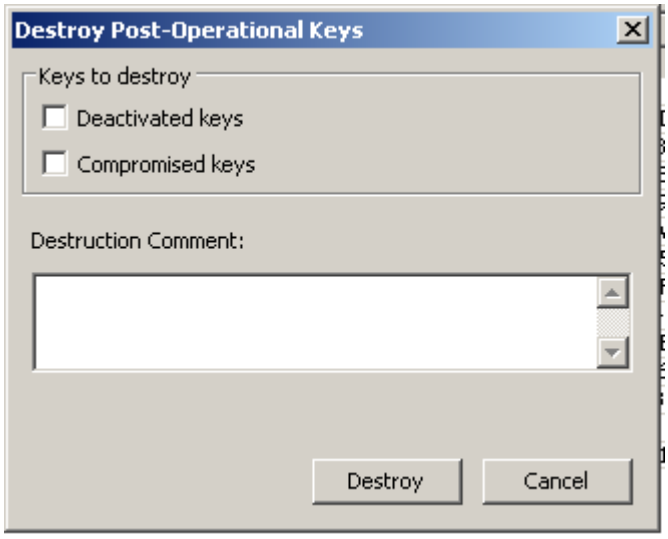
バックアップファイルがダウンロードされた日時が表示されます。

4. 「**Save**」ボタンをクリックして変更を保存します。

運用後鍵の破棄

データユニットに関連付けられている運用後鍵を破棄するには、次の手順を実行します。

1. 「Data Unit List」画面から、破棄するデータユニットを強調表示し、「**Destroy Keys**」ボタンをクリックします。
2. 次のように、破棄する鍵の指定を求めるダイアログボックスが表示されます。



Deactivated keys

鍵の暗号有効期間が過ぎているが、情報を処理 (復号化) するために鍵が必要となる可能性がある場合には、このチェックボックスを選択します。

Compromised keys

承認されていない実体に鍵が渡された場合、または承認されていない実体によって鍵が検出された場合に鍵を破棄するには、このチェックボックスを選択します。

Destruction Comment

これらの鍵の破棄に関するコメントを入力します。

3. 「**Destroy**」ボタンをクリックすると、これらの鍵の破棄を確認する別のダイアログボックスが表示されます。
4. 「**Yes**」ボタンをクリックします。破棄した鍵の数を示す別のダイアログボックスが表示されます。

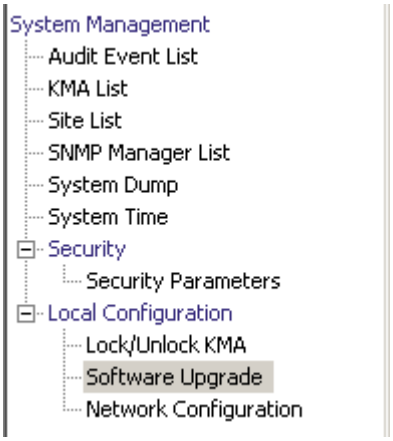
「Software Upgrade」メニュー

「Software Upgrade」メニューオプションを使用すると、オペレータは、ソフトウェアアップグレードプロセスの次の最初のフェーズを実行できます。

- ソフトウェアアップグレードファイルを KMA にアップロードする
- アップグレードをただちに適用する

> **注 ー このプロセスの 2 番目のフェーズ (ソフトウェアバージョンのアクティブ化) は、セキュリティー責任者が実行する必要があります。詳細は、226 ページの「ソフトウェアのアップグレード」を参照してください。**

ソフトウェア更新は Oracle によって署名され、適用前に KMA によって検証されます。



ソフトウェアアップグレードの実装のガイドライン

- この機能を実行する前に、システムをバックアップしてください。手順については、329 ページの「バックアップの作成」を参照してください。
- OKM Manager の GUI リリースは、KMA に読み込むアップグレードのバージョンと一致するものを使用してください。
- KMS 2.1 以前を実行している KMA を OKS 2.3 以降にアップグレードするには、まずその KMA を KMS 2.2 にアップグレードする必要があります。
- OKM Manager が KMA にリモート接続しているか、または OKM Manager と KMA の間の接続が低速な場合、アップロードと適用の処理に時間がかかる可能性があります。これを軽減するために、OKM Manager がインストールされているノートパソコンまたはワークステーション、および、KMA と同じサブネットに接続しているノートパソコンまたはワークステーションに、ソフトウェアアップグレードファイルをダウンロードできます。OKM Manager と KMA の間にルーターがある場合、アップグレード処理の速度が低下する場合があります。
- アップロードと適用の処理には、OKM Manager と KMA 間の接続環境が良好な場合でも、最短で約 30 分以上かかります。アクティブ化処理には、最短でも 5 - 15 分かかります。アップロード処理があまりに低速な場合、同じサブネットに KMA として接続してみてください。

- (ネットワーク負荷の分散を促進するために) 各 KMA にソフトウェアアップグレードファイルを一度に 1 つずつアップロードおよび適用してから、(同時にオフラインになる KMA の数を最小化するために) 各 KMA で一度に 1 つずつソフトウェアアップグレードをアクティブ化してください。
- いずれかのアップグレード処理 (アップロード、検証、適用、アクティブ化、複製バージョンの切り替え) が失敗した場合、OKM Manager は、失敗の理由と提案する解決方法を説明する監査メッセージを生成します。
- アップグレードされた KMA では技術サポートアカウントが使用不可になっており、必要な場合はアカウントをふたたび使用可能にする必要があります。

ソフトウェアアップグレードのアップロードおよび適用

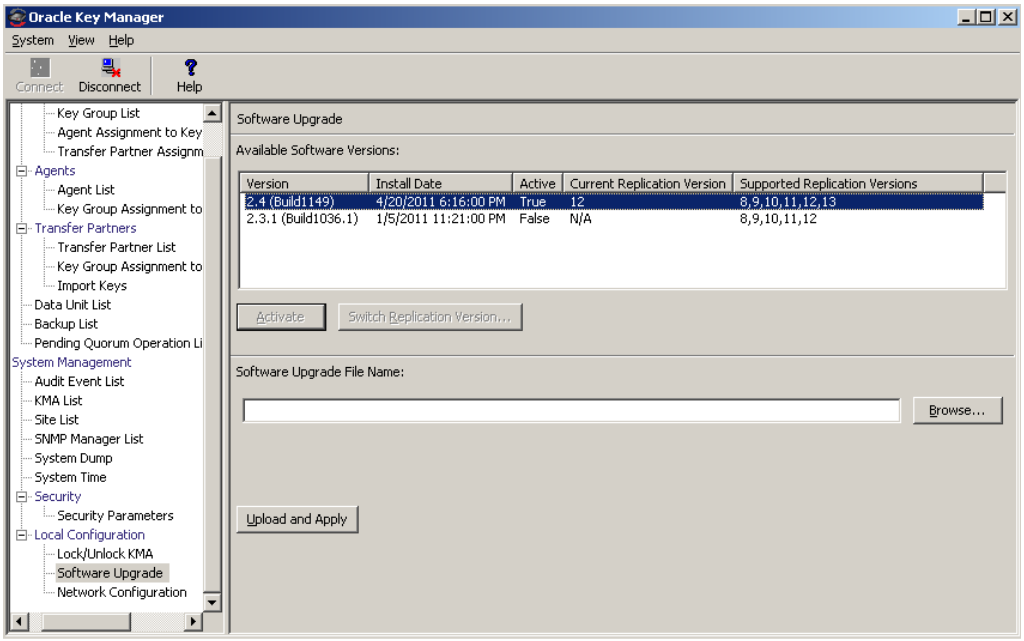
ソフトウェアアップグレードプロセスの最初のフェーズは、ソフトウェアアップグレードファイルのアップロードと適用です。

1. ソフトウェアアップグレードファイルを配信場所から PC またはワークステーションにダウンロードします。バージョンはファイル名に示されています。

   注 ー このファイルを、OKM Manager GUI から移動できる場所に保存します。

2. 「Local Configuration」メニューから、「**Software Upgrade**」を選択します。「Software Upgrade」画面が表示されます。

   ソフトウェアのアクティブなバージョンが強調表示され、「Active」列が「True」に設定され、アクティブでないバージョンが表示されます。



この画面には次のボタンが表示されます。

有効

セキュリティー責任者は、アクティブでないソフトウェアバージョンを選択し、このボタンをクリックして選択されたソフトウェアバージョンをアクティブにできます。このソフトウェアバージョンがアクティブ化されることを知らせるメッセージが表示され、KMA が再起動します。

Switch Replication Version

セキュリティー責任者は、アクティブなソフトウェアバージョンを選択し、このボタンをクリックして現在の複製バージョンを切り替えることができます。

Software Upgrade File Name

ソフトウェアアップグレードファイルの名前を入力します。

参照

ローカルシステム上のソフトウェアアップグレードファイルを見つけるには、このボタンをクリックします。

Upload and Apply

アップロードおよび適用プロセスを開始するには、このボタンをクリックします。ソフトウェアアップグレードファイルがいつアップロードされ、いつ適用されたを示すメッセージが表示されます。

3. 「Software Upgrade File Name」フィールドに、ソフトウェアアップグレードファイルの名前を入力します。また、「**Browse**」ボタンを選択してファイルを見つけることもできます。「**Upload and Apply**」ボタンをクリックします。

   OKM はアップロード、確認、および適用プロセスを開始し、プロセスがどの手順にあるかを示す処理進捗インジケータを表示します。

   注 ー アップロードプロセスによってネットワークに一定のトラフィックが追加されるため、ビジー状態にあるクラスタでは KMA を同時にアップロードしないようにすることをお勧めします。

ソフトウェアバージョンのアクティブ化

ソフトウェアアップグレードプロセスの 2 番目のフェーズは、アップロードして適用したアクティブでないソフトウェアバージョンのアクティブ化です。セキュリティー責任者は、この処理を実装する必要があります。詳細については、226 ページの「ソフトウェアのアップグレード」を参照してください。

「Backup List」メニュー

バックアップファイルの詳細情報の表示手順については、325 ページの「「Backup List」メニュー」を参照してください。

「Audit Event List」メニュー

監査イベントリストの表示手順については、281 ページの「「Audit Event List」メニュー」を参照してください。

「KMA List」メニュー

KMA のリストの表示手順については、119 ページの「「KMA List」メニュー」を参照してください。

「Site List」メニュー

サイトのリストの表示手順については、152 ページの「「Site List」メニュー」を参照してください。

「SNMP Manager List」メニュー

SNMP Manager のリストの表示手順については、160 ページの「「SNMP Manager List」メニュー」を参照してください。

「System Time」メニュー

KMA の時刻を表示する手順については、233 ページの「Level of Telemetry Data」を参照してください。

「Lock/Unlock KMA」メニュー

KMA のロック状態を表示する手順については、222 ページの「Lock/Unlock KMA」を参照してください。

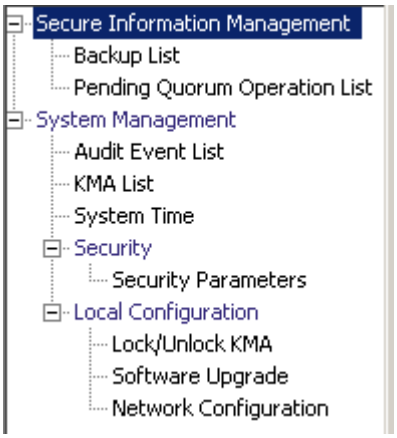
8

バックアップオペレータの操作

この章では、バックアップオペレータの役割を付与されたユーザーが実行できる操作について説明します。ほかの役割が割り当てられている場合は、その役割の実行手順について、該当する章を参照してください。

バックアップオペレータの役割

バックアップオペレータは、データおよびその鍵のセキュリティー保護および格納を担当します。



「Backup List」メニュー

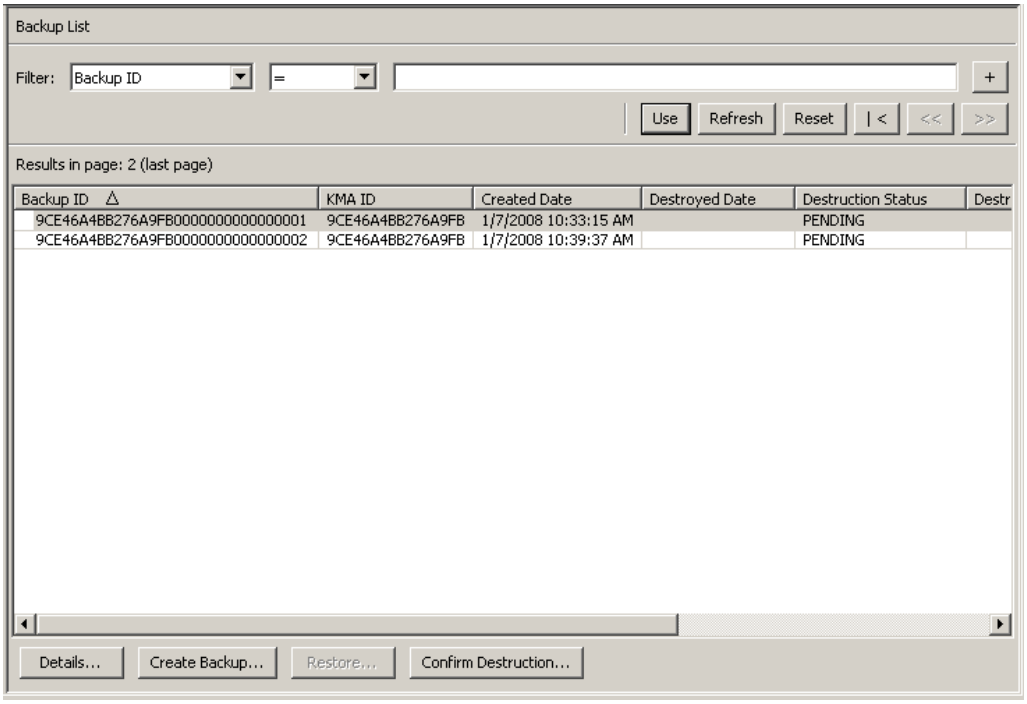
「Backups List」メニューオプションを使用すると、バックアップオペレータは次の操作を実行できます。

- バックアップ履歴の表示およびバックアップ破棄ステータスの確認
- バックアップの作成

バックアップファイルの履歴の表示

バックアップファイルの履歴を表示するには、次の手順を実行します。

「Backups」メニューから「**Backup List**」を選択します。「Backup List」画面が表示されます。



バックアップに関する詳細情報を表示する場合は、そのバックアップを強調表示して「**Details**」ボタンをクリックします。詳細については、「バックアップの詳細の表示」を参照してください。

バックアップを作成するには、「**Create Backup**」ボタンをクリックします。詳細については、329 ページの「バックアップの作成」を参照してください。

バックアップの破棄を確認するには、「**Confirm Destruction**」ボタンをクリックします。詳細については、330 ページの「バックアップの破棄の確認」を参照してください。

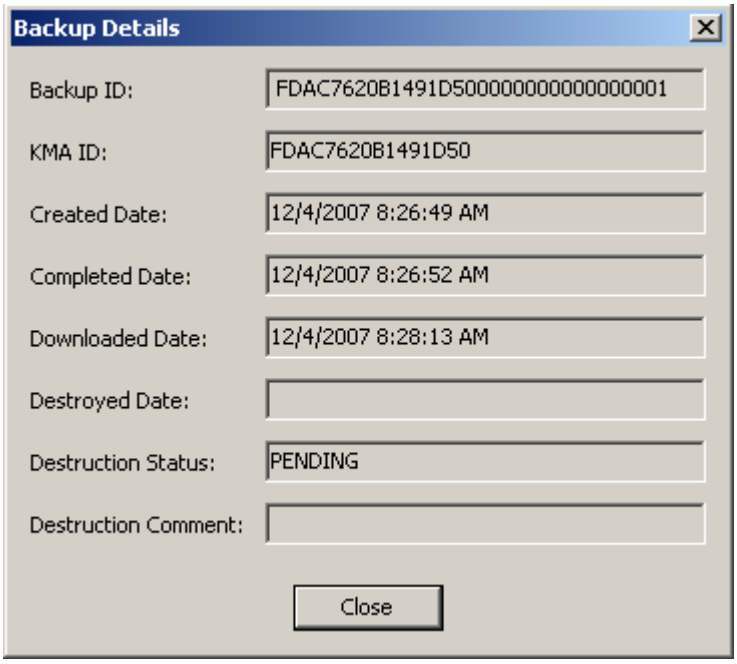
バックアップの詳細の表示

「Backup Details」ダイアログボックスは、バックアップファイルの詳細を表示する場合に使用します。

> **注 ー** バックアップファイルは、そのバックアップが作成されるときに OKM Manager が実行されていたマシンにダウンロードされます。

バックアップファイルの詳細を表示するには、次の手順を実行します。

1. 「Backups List」画面で、詳細情報を表示するバックアップエントリをダブルクリックするか、またはバックアップエントリを強調表示して「**Details**」ボタンをクリックします。「Backup Details」ダイアログボックスが表示されます。すべてのフィールドが使用不可になっています。



2. 次に、フィールドとその説明を示します。

Backup ID

各バックアップファイルを識別する一意のシステム生成識別子が表示されます。

KMA ID

このバックアップファイルが生成された KMA が表示されます。

作成日

バックアップファイルが作成された日時が表示されます。

Completed Date

バックアップファイルの作成が完了した日時が表示されます。

Downloaded Date

バックアップファイルがダウンロードされた日時が表示されます。

Destroyed Date

バックアップファイルが破棄された日付が表示されます。

Destruction Status

破棄に関するバックアップの状態が表示されます。

Destruction Comment

バックアップファイルの破棄に関するユーザー指定の情報が表示されます。

3. このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。

バックアップの作成

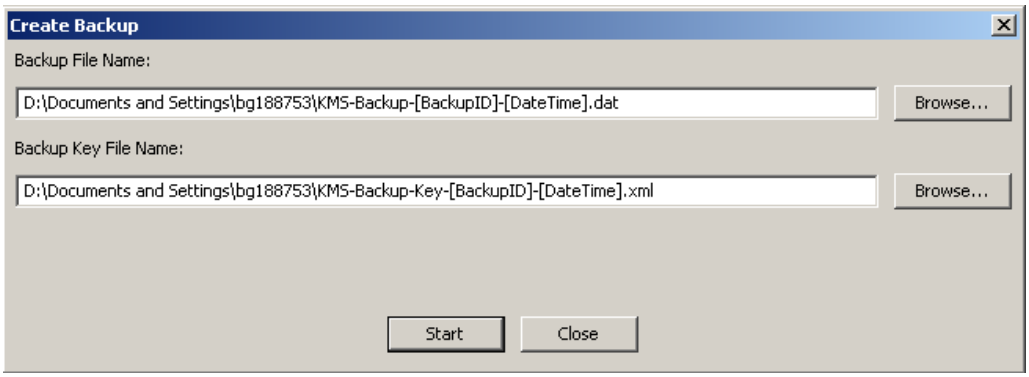
重要 ― バックアップ責任者がバックアップを作成できるようにするには、セキュリティー責任者が事前にコアセキュリティー鍵データをバックアップしておく必要があります。214 ページの「コアセキュリティーバックアップの作成」を参照してください。

常に、KMA には、バックアップファイルと復元ファイルがそれぞれ 1 つのみ存在します。

このオプションを使用すると、バックアップファイルとバックアップ鍵ファイルという 2 つのファイルで構成されたバックアップを作成できます。

バックアップを作成するには、次の手順に従います。

1. 「Backup List」画面から、「**Create Backup**」ボタンをクリックします。「Create Backup」ダイアログボックスが表示されます。



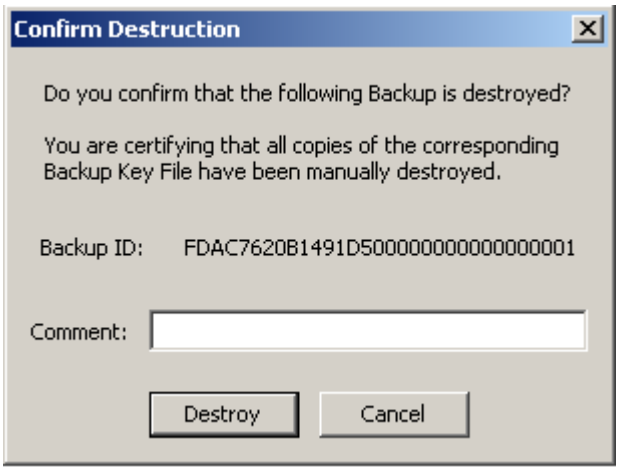
注 ー バックアップファイルおよびバックアップ鍵ファイルの名前が自動的に生成されます。ただし、名前は編集できます。また、「Browse」ボタンをクリックして宛先パスを選択することもできます。

2. 「**Start**」ボタンをクリックしてバックアップファイルを作成し、バックアップ鍵ファイルをユーザー指定の宛先にダウンロードします。
3. バックアップが完了すると、このことを示すメッセージが表示されます。このダイアログボックスを閉じるには、「**Close**」ボタンをクリックします。
4. 「Backup List」画面が再度表示されます。新しく作成したバックアップファイルが表示されています。

バックアップの破棄の確認

バックアップの破棄を確認するには、次の手順に従います。

1. 「Backup List」画面から、破棄するバックアップを強調表示し、「**Confirm Destruction**」ボタンをクリックします。次のダイアログボックスが表示され、選択したバックアップの破棄ステータスの更新することが確認されます。処理を続行する前に、対応するバックアップ鍵ファイルのすべてのコピーが手動で破棄されていることを確認してください。



2. 対応するバックアップ鍵ファイルのすべてのコピーが手動で破棄されたことが確実である場合は、「**Yes**」ボタンをクリックします。それ以外の場合は、「**No**」ボタンをクリックしてプロセスを停止します。
3. 「**Yes**」ボタンを選択した場合は、バックアップとそれに関連付けられたデータユニットが「完全に破棄」されます。

「KMA List」メニュー

「KMA List」メニューオプションを使用すると、次の操作を行うことができます。

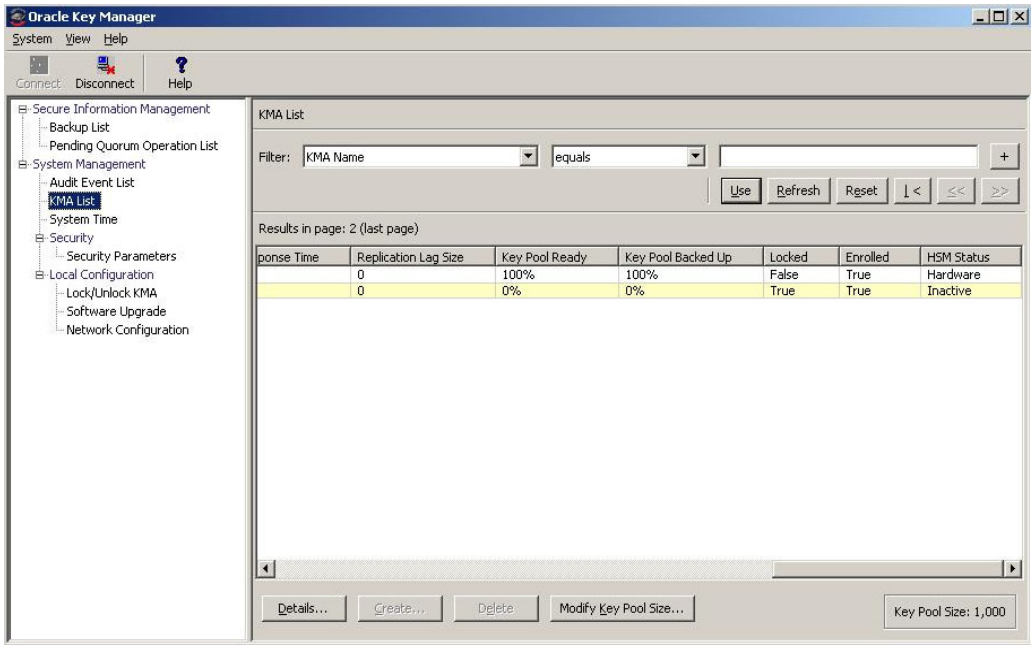
- KMA の表示 (120 ページの「KMA の表示」を参照)
- KMA の作成 (126 ページの「KMA の作成」を参照)
- KMA の情報の変更 (129 ページの「KMA の詳細の表示および変更」を参照)
- KMA の削除 (135 ページの「KMA の削除」を参照)
- 鍵プールサイズの変更

> **注 ー** バックアップオペレータは KMA の詳細の表示や、鍵プールサイズの変更を行うことができます。

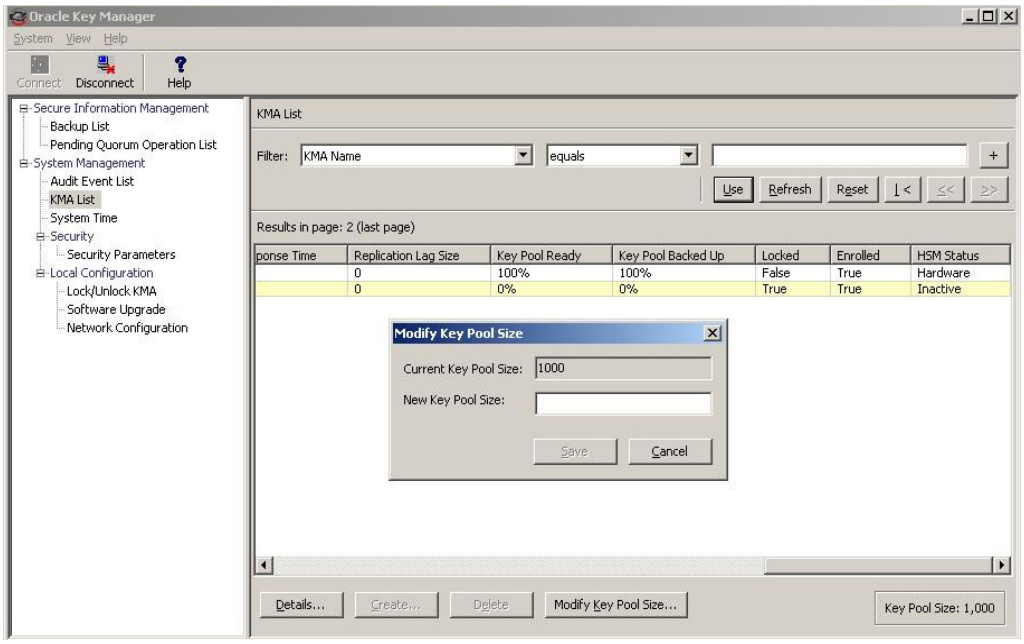
鍵プールサイズの変更

鍵プールサイズを変更するには、次の手順を実行します。

1. 「System Management」メニューから、「**KMA List**」を選択します。「KMA List」画面の右側が、次のように表示されます。



2. 「**Modify Key Pool Size**」をクリックします。次の画面が表示されます。



3. 新しい鍵プールサイズを指定します。

その他の機能

バックアップオペレータは、次の操作を行うことができます。

- 監査イベントリストの表示
- システム時刻の表示
- KMA のロックステータスの表示

監査ログの表示手順については、281 ページの「「Audit Event List」メニュー」を参照してください。

KMA の時刻を表示する手順については、233 ページの「Level of Telemetry Data」を参照してください。

KMA のロック状態を表示する手順については、222 ページの「Lock/Unlock KMA」を参照してください。

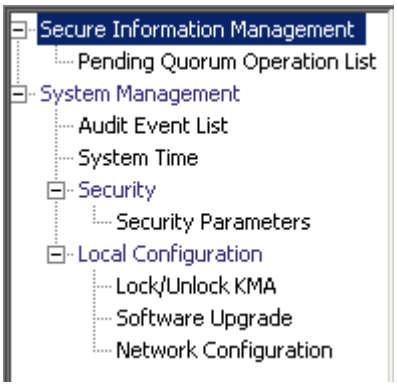
9

監査者の操作

この章では、監査者の役割を付与されたユーザーが実行できる操作について説明します。ほかの役割が割り当てられている場合は、その役割の実行手順について、該当する章を参照してください。

監査者の役割

監査者は、「Audit List」イベントと KMA を表示できます。



「Audit List」メニュー

「Audit List」メニューの使用手順については、281 ページの「「Audit Event List」メニュー」を参照してください。

「Security Parameters」メニュー

「Security Parameters List」メニューを使用すると、監査者は KMA のセキュリティーパラメータを表示できます。「Security Parameters」メニューの使用手順については、206 ページの「「Security Parameters」メニュー」を参照してください。

その他の機能

監査者は、次の操作を行うこともできます。

- KMA のロックおよびロック解除のステータスの表示
- システム時刻の表示

KMA のロックおよびロック解除のステータスの表示手順については、222 ページの「Lock/Unlock KMA」を参照してください。

KMA の時刻の調整手順については、233 ページの「Level of Telemetry Data」を参照してください。

インストールされているソフトウェアのバージョンの表示手順については、321 ページの「「Software Upgrade」メニュー」を参照してください。

10

定足数メンバーの操作

この章では、定足数メンバーの役割が割り当てられたユーザーが実行できる操作について説明します。ほかの役割が割り当てられている場合は、その役割の実行手順について、該当する章を参照してください。

定足数メンバーの役割

定足数メンバーの役割は、保留中の定足数操作を表示および承認します。

最初に、セキュリティーオペレータの役割が割り当てられたユーザーが OKM Manager の GUI にログインし、1 名以上のユーザーを作成し、定足数メンバーの役割を割り当てる必要があります (140 ページの「ユーザーの作成」を参照)。

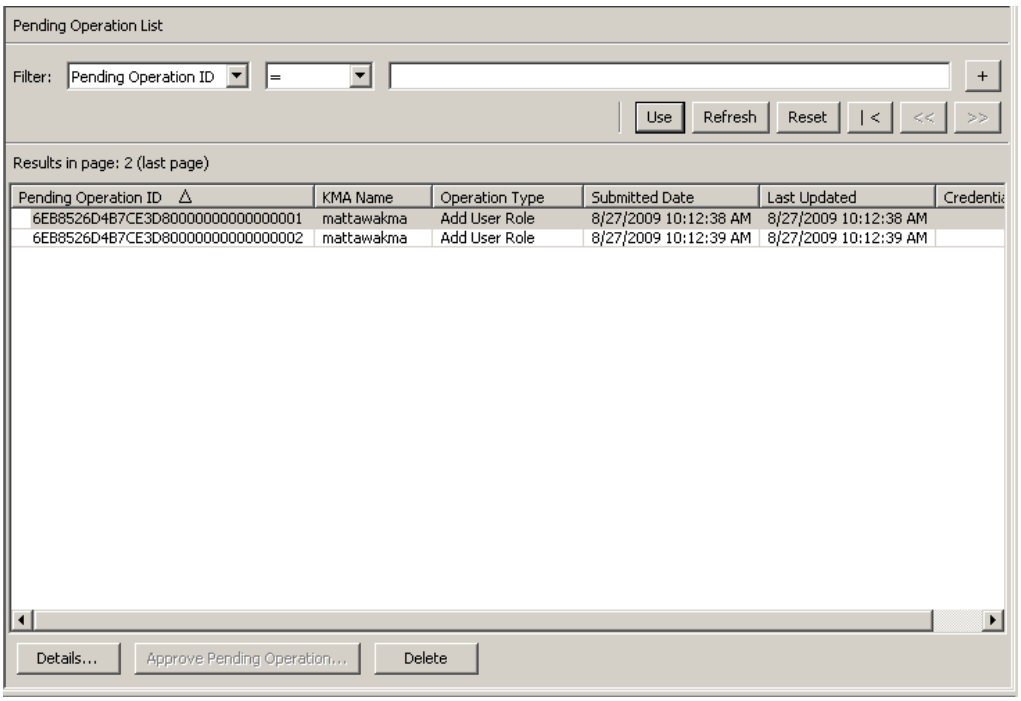
すべての定足数メンバーユーザーが作成済みとは限らないため、定足数メンバーの役割を持つユーザーを作成するとき、セキュリティー責任者は「Key Split Quorum Authentication」ダイアログで十分な定足数の鍵分割資格を指定する必要があります。

「Pending Quorum Operation List」メニュー

「Pending Quorum Operation List」メニューは、システムでその操作を実行する前に、定足数の鍵分割資格の承認が必要な保留中の操作をすべて表示します。このメニューは、ユーザーが定足数メンバーまたはセキュリティー責任者の役割を持つ場合に表示されます。

「Pending Quorum Operation List」メニューには、次の操作のためのオプションがあります。

- 保留中の操作リストの詳細の表示
- 保留中の操作の承認
- 保留中の操作の削除



次のいずれかのキーで、保留中の操作リストにフィルタを適用できます。

- Pending Operation ID
- KMA 名
- Operation Type
- Submitted Date
- Last Updated

表示されている保留中の操作リストにフィルタを適用するには、「**Use**」ボタンを使用します。

次に、フィールドとその説明を示します。

フィルタ :

KMA へのクエリーの結果にフィルタを適用するために使用できるフィールドが表示されます。取り得る値は次のとおりです。

- Pending Operation ID
- KMA 名
- Operation Type
- Submitted Date
- Last Updated

フィルタ演算子ボックス :

下矢印ボタンをクリックし、必要なフィルタ演算子を選択します。取り得る値は次のとおりです。

- 等しい =
- 等しくない <>
- より大きい >
- より小さい <
- 大きいか等しい >=
- 小さいか等しい <=
- 開始 ~
- 空白
- 空白以外

フィルタ値テキストボックス :

選択した属性のフィルタ条件として使用する値を入力します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

フィルタ値コンボボックス :

下矢印ボタンをクリックし、選択した属性のフィルタ条件として使用する値を選択します。フィルタ属性によっては、このフィルタオプションが表示されない場合もあります。

このボタンをクリックすると、フィルタが追加されます。

このボタンをクリックすると、フィルタが削除されます。このボタンは、複数のフィルタが表示されている場合にのみ表示されます。

使用 :

このボタンをクリックすると、表示されているリストに選択したフィルタが適用され、リストの最初のページが表示されます。

更新 :

このボタンをクリックすると、リストが再表示されます。

リセット :

このボタンをクリックすると、すべてのフィルタが削除され、表示されているリストがリセットされて最初のページが表示されます。

このボタンをクリックすると、リストの最初のページに移動します。

このボタンをクリックすると、前のページに移動します。

このボタンをクリックすると、次のページに移動します。

Results in Page:

「Options」ダイアログボックスの「Query Page Size」フィールドで設定した 1 ページ当たりのレコード数が表示されます。

Pending Operation ID:

保留中の定足数操作を一意に識別します。

KMA Name:

この操作が実行された KMA の名前。

Operation Type:

定足数操作の種類。

Submitted Date:

保留中の定足数操作が実行された日付。

Last Updated:

この操作の定足数が最後に更新された日付。保留中である特定の定足数操作の定足数は、新たな定足数メンバーが鍵分割ユーザー名を指定し、その操作を承認するたびに更新されます。保留中の定足数操作について、保留中操作の資格の有効期間内に十分な数の鍵分割ユーザーがその操作を承認しないと、操作は期限切れになります。この日付は当初、保留中の定足数操作が実行された日付と同じ日付に設定されます。

Credentials:

この保留中の定足数操作をすでに承認した鍵分割ユーザー名のリスト。

詳細 :

保留中の定足数操作の詳細情報を表示するには、このボタンをクリックします。

Approve Pending Operation:

保留中の定足数操作を承認するには、このボタンをクリックします。この操作を行うには、定足数メンバーの役割が必要です。

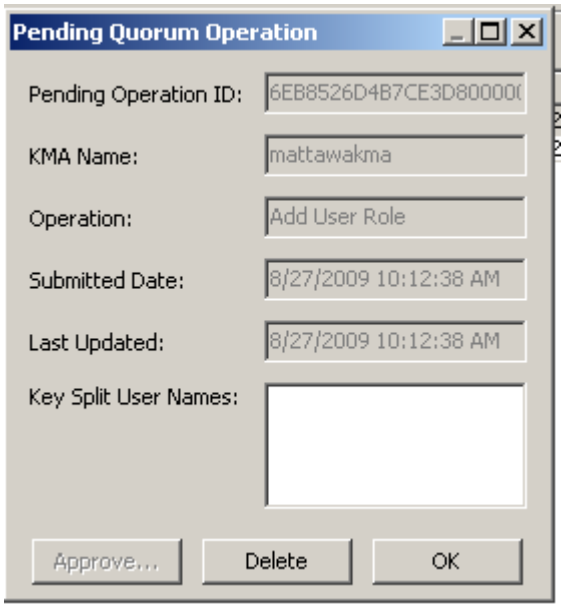
Delete:

選択した保留中の定足数操作を削除するには、このボタンをクリックします。この操作を行うには、セキュリティー責任者の役割が必要です。

保留中操作の詳細の表示

保留中の操作の詳細を表示するには、次の手順を実行します。

「Pending Operation List」画面で、「**Details**」ボタンをクリックします。「Pending Quorum Operation」ダイアログボックスが表示されます。



すでにこの操作を承認した鍵分割ユーザーがいる場合、「Key Split User Names」フィールドに一覧表示されます。

「Audit Event List」パネルに表示されている監査イベントにフィルタを適用すると、特定の保留中の定足数操作についての詳細な情報を得ることができます (282 ページの「監査ログの表示」を参照)。

1. 「Audit Event List」パネルに移動します。
2. 「Add Pending Quorum Operation」に設定された「Operation」フィルタを使用してフィルタを定義します。保留中の定足数操作が複数ある場合、「Created Date」を使用して別のフィルタを定義し、この特定の保留中の定足数操作が実行された日付を含む期間を指定できます。
3. このフィルタ条件を満たす監査イベントを表示するには、「**Use**」ボタンを使用します。フィルタが適用された監査イベントの「Message Values」フィールドに、保留中の定足数操作についての詳細情報が表示されます。

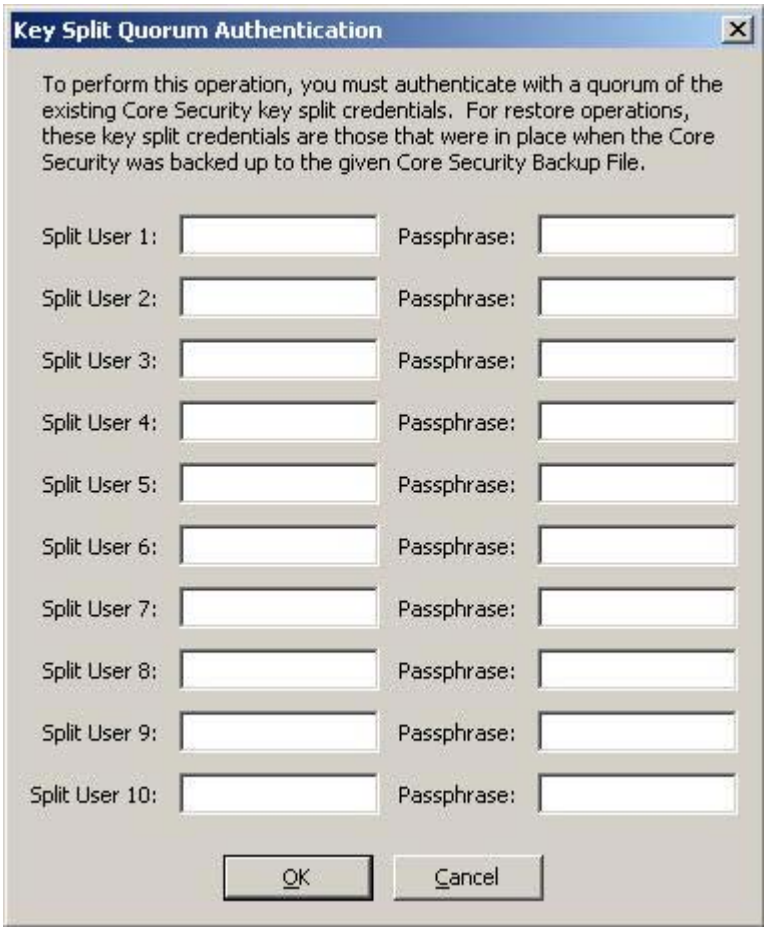
保留中の定足数操作の承認

保留中の操作を承認するには、定足数メンバーの役割で OKM Manager の GUI にログインする必要があります。それ以外の場合、「**Approve**」ボタンは使用不可になっています。

定足数メンバーの役割を持つほかのユーザーも個別にログインし、保留中の定足数操作を承認できます。十分な定足数の鍵分割資格が保留中の定足数操作を承認すると、OKM クラスタはその操作を実行します。

保留中の定足数操作を承認するには、次の手順を実行します。

1. 「Pending Operation List」画面で、「**Approve Pending Operation**」ボタンをクリックします。
2. 「Key Split Quorum Authentication」ダイアログボックスが表示されます。



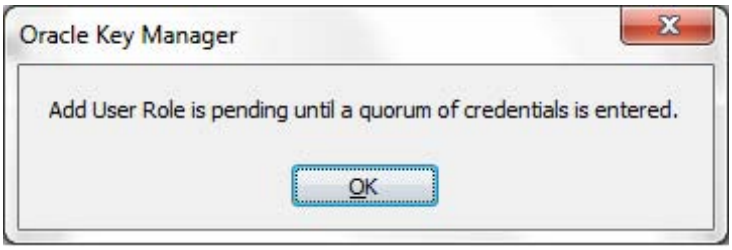
「Key Split Quorum Authentication」ダイアログボックスで鍵分割資格の十分な定足数を指定した場合、「**保存**」ボタンをクリックしたときではなく、定足数を指定したあとに OKM クラスタで情報が更新されます。

「Key Split Quorum Authentication」ダイアログボックスで十分な定足数を指定しない場合、複製バージョンに応じて 2 つの異なる結果になる可能性があります。

複製バージョン：	**結果：**
10 またはそれ以下	操作は失敗し、OKM クラスタではどの情報も更新されません。
11 以降	操作は保留状態になります。システムは、保留中の定足数操作のリストに操作を追加します (338 ページの「「Pending Quorum Operation List」メニュー」を参照)。このリストに操作が追加されると、ポップアップメッセージが表示されます。 定足数メンバーの役割を持つユーザー (定足数メンバーユーザー) がログインし、十分な定足数を指定するまでは、OKM クラスタでどの情報も更新されません。

3. 操作を認証するには、定足数ユーザーの名前とパスフレーズを入力します。

   十分な定足数の鍵分割資格をただちに指定しない場合、システムは保留中の定足数操作のリストに操作を追加し、次のダイアログボックスを表示します。



「**OK**」をクリックすると、「Pending Quorum Operation List」画面にこの操作が表示されます (338 ページの画面例を参照)。

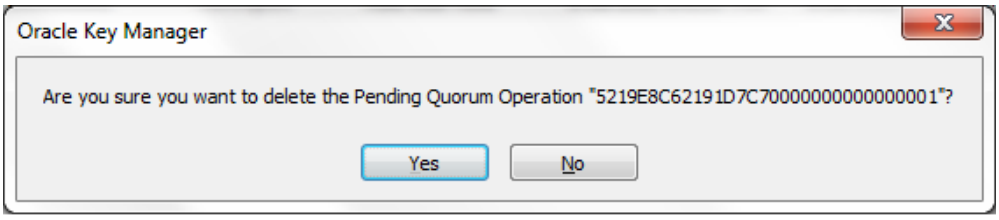
保留中の定足数操作の削除

保留中の操作を削除するには、セキュリティー責任者の役割で OKM Manager の GUI にログインする必要があります。それ以外の場合、「**Delete**」ボタンは使用不可になっています。

保留中の操作を削除するには、次の手順を実行します。

1. 「Pending Operation List」画面で、削除する保留中の操作を強調表示して「**Delete**」ボタンをクリックします。

   次のように、選択した保留中の操作の削除を確認するダイアログボックスが表示されます。



2. 「**Yes**」ボタンをクリックして、保留中の操作を削除します。現在選択している保留中の操作が削除され、「Pending Operation List」画面に戻ります。また、保留中の操作に関連付けられていたエントリもすべて削除されます。

関連操作

次の操作には、定足数の鍵分割資格が必要です。

- 126 ページの「KMA の作成」
- 133 ページの「KMA のパスフレーズの設定」
- 140 ページの「ユーザーの作成」
- 143 ページの「ユーザーの詳細の表示および変更」
- 145 ページの「ユーザーのパスフレーズの設定」
- 179 ページの「転送パートナーの作成」
- 183 ページの「転送パートナーの詳細の表示および変更」
- 201 ページの「バックアップの復元」
- 219 ページの「Autonomous Unlock Option」
- 222 ページの「Lock/Unlock KMA」
- 322 ページの「ソフトウェアアップグレードのアップロードおよび適用」

11

OKM コンソールの使用法

この章では、OKM コンソールのオプションについて説明します。

OKM コンソールの概要

OKM コンソールは端末テキストベースのインタフェースで、これを使用すると、KMA の基本的な機能を設定できます。KMS コンソールには、ビデオモニターとキーボードを KMA に物理的に接続してアクセスするか、または ELOM の Web ブラウザインタフェース (40 ページの「サービスプロセッサを介した KMA へのアクセス」を参照) の「リモートコンソール」機能によってアクセスします。

KMA が起動し、ユーザーがこれを終了できなかった場合に、オペレーティングシステムによって OKM コンソールが自動的に起動されます。ユーザーに割り当てられた役割によって、OKM コンソールのオプションは異なります。

OKM コンソールにログインするには、OKM Manager でユーザーアカウントを作成する必要があります。OKM コンソールにログインするには、OKM での認証に使用されたものと同じユーザー名およびパスフレーズを使用する必要があります。

> **注 ー** QuickStart プログラムを起動すると、最初のセキュリティー責任者のアカウントだけが作成されます。

KMA へのログイン

KMA の起動後、次の情報が表示されます。

```
Copyright (c) 2007, 2011, Oracle and/or its affiliates. All
rights reserved.
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Please enter your User ID:
```

1. プロンプトで、ユーザー名を入力して Enter キーを押します。
2. 「`Please enter your Passphrase:`」プロンプトで、パスフレーズを入力して Enter キーを押します。ユーザーに割り当てられた役割によって、OKM コンソールのオプションは異なります。メニューには、KMA のバージョンおよびログオンしているユーザーが表示されます。

ユーザーの役割の操作については、以降のページで説明します。これには、次の役割が含まれます。

- オペレータ (352 ページの「オペレータの役割の機能」を参照)
- セキュリティー責任者 (359 ページの「セキュリティー責任者の役割の機能」を参照)
- その他の役割 (381 ページの「その他の役割の機能」を参照)

オペレータ

次のメニューには、オペレータの役割に関するオプションが示されています。

KMA のシリアル番号は、「Auto Service Request」機能が有効な場合に表示されます。この例では、0710QAL0CF です。233 ページの「ASR (Auto Service Request)」および 37 ページの「ASR (Auto Service Request) 機能」を参照してください。

KMA が Sun Fire X2100 M2 または X2200 M2 サーバーである場合、このシリアル番号は、オラクルの担当者が使用する権利付与パーツ番号とは異なります。

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Please enter your User ID: OP
Please enter your Passphrase:

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------
(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
------------------------------------------------------------
Please enter your choice:
```

セキュリティー責任者

次のメニューには、セキュリティー責任者の役割に関するオプションが示されています。

KMA のシリアル番号は、「Auto Service Request」機能が有効な場合に表示されます。この例では、0710QAL0CF です。233 ページの「ASR (Auto Service Request)」および 37 ページの「ASR (Auto Service Request) 機能」を参照してください。

KMA が Sun Fire X2100 M2 または X2200 M2 サーバーである場合、このシリアル番号は、オラクルの担当者が使用する権利付与パーツ番号とは異なります。

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Please enter your User ID: SO
Please enter your Passphrase:

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------
(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

注 ー ユーザーにオペレータとセキュリティーの両方の役割が割り当てられている場合、メニューオプションは次のように組み合わせて表示されます。

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Please enter your User ID: SO
Please enter your Passphrase:

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------

(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

その他の役割

その他すべての役割 (バックアップオペレータ、コンプライアンス責任者、監査者、および定足数メンバー) では、次のようなメニューが表示されます。使用可能なオプションは、KMA からのログアウトとキー配列の設定のみです。

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------

(1)  Set Keyboard Layout
(0)  Logout

------------------------------------------------------------
Please enter your choice:
```

オペレータの役割の機能

この節では、オペレータが実行できる機能について説明します。次の機能があります。

- KMA の再起動 (353 ページ)
- KMA の停止 (354 ページ)
- 技術サポートの無効化 (355 ページ)
- 主管理者の無効化 (356 ページ)
- キー配列の設定 (357 ページ)
- KMA からのログアウト (358 ページの「ログアウト」ページ)

オペレータのメニューは次のとおりです。

```
Oracle Key Manager Version (build1179)
------------------------------------------------------------
Please enter your User ID: SO
Please enter your Passphrase:

Oracle Key Manager Version (build1179) -- OP on glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------

(1)  Reboot KMA
(2)  Shutdown KMA
(3)  Technical Support
(4)  Primary Administrator
(5)  Set Keyboard Layout
(0)  Logout
------------------------------------------------------------
Please enter your choice:
```

注 ー 技術サポートおよび主管理者のメニュー項目は、それらの設定が現在有効になっている場合にのみ表示されます。

KMA の再起動

「Reboot KMA」メニューオプションを使用すると、オペレータが、KMA を停止および再起動して、オペレーティングシステムを再起動することができます。この機能は、障害追跡のみに使用します。

KMA を再起動するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**1** を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Reboot KMA
------------------------------------------------------------
Press Ctrl-c to abort.
Are you sure that you want to reboot the KMA? [y/n]: y
```

2. プロンプトで、**y** を入力して Enter キーを押します。KMA の再起動が開始されると、現在の OKM コンソールセッションが終了します。KMA の再起動後、OKM コンソールのログインプロンプトが表示されます。

KMA の停止

このオプションを使用すると、KMA のすべてのサービスを終了 (停止) して、KMA 自体を物理的に停止することができます。

> **注 ー** 数時間以上にわたって KMA が停止されており、自律ロック解除オプションが有効になっている場合は、KMA を再起動する前に KMA をロックしてください。
>
> 「KMA List」パネルで「Replication Lag Size」によって示されるように、最近の更新がこの KMA に伝播されたあとに KMA をロック解除してください。
>
> 詳細は、次の各項目を参照してください。
>
> - 219 ページの「Autonomous Unlock Option」
> - 222 ページの「Lock/Unlock KMA」
> - 119 ページの「「KMA List」メニュー」

KMA を停止するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**2** を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Shutdown KMA
------------------------------------------------------------
Press Ctrl-c to abort
Are you sure that you want to shut down the KMA? [y/n]: y
```

2. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、システムの停止中であることが示されます。

```
Shutting down...
```

3. 停止処理が表示されます。停止処理が完了すると、次の情報が表示されます。

```
Power down
```

4. KMA の電源が切断されました。電源ボタンまたは ELOM の遠隔電源制御機能のいずれかを使用して、KMA の電源を入れることができます。

技術サポートアカウントの無効化

注 ー このタスクの有効化はセキュリティー責任者のみが実行できます。無効化はオペレータまたはセキュリティー責任者が実行できます。

技術サポートアカウントを無効にするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**3** を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently ENABLED.

Would you like to DISABLE the support account? [y/n]: y
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE the support account?
[y/n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。SSH サービスは自動的に停止します。

主管理者の無効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

> **注 ー** このタスクの有効化はセキュリティー責任者のみが実行できます。無効化はオペレータまたはセキュリティー責任者が実行できます。

主管理者のアクセスの無効化は即時に実行されます。別のユーザーが主管理者として接続している場合に、このアクセスを無効にすると、そのユーザーが次に実行しようとしたコマンドは失敗します。

1. 主管理者のアクセスを無効にするには、次の手順を実行します。

メインメニューの「`Please enter your choice:`」プロンプトで、**4** を入力して Enter キーを押します。次の情報が表示され、アクセスが有効であることが示されます。

```
Primary Administrator
------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。主管理者のアクセスが無効になりました。

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

> **注 ー** 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、**5** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian       ( 2) Belarusian    ( 3) Belgian
( 4) Bulgarian      ( 5) Croatian      ( 6) Danish
( 7) Dutch          ( 8) Finnish       ( 9) French
(10) German         (11) Icelandic     (12) Italian
(13) Japanese-type6 (14) Japanese      (15) Korean
(16) Malta_UK       (17) Malta_US      (18) Norwegian
(19) Portuguese     (20) Russian       (21) Serbia-And-Montenegro
(22) Slovenian      (23) Slovakian     (24) Spanish
(25) Swedish        (26) Swiss-French  (27) Swiss-German
(28) Taiwanese      (29) TurkishQ      (30) TurkishF
(31) UK-English     (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「Please enter the number for the keyboard layout:」プロンプトで、キー配列を変更する番号を入力します。新しいキー配列が適用されます。
3. 次の情報が表示されます。Press Enter to continue.

ログアウト

現在の OKM コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、OKM コンソールにふたたびログインできます。

セキュリティー責任者の役割の機能

この節では、セキュリティー責任者が実行できる機能について説明します。次の機能があります。

- KMA のクラスタへのログイン (360 ページ)
- ユーザーのパスフレーズの設定 (362 ページ)
- KMA の管理 IP アドレスの設定 (364 ページ)
- KMA のサービス IP アドレスの設定 (366 ページ)
- ゲートウェイ設定の変更 (368 ページ)
- DNS 設定の指定 (370 ページ)
- KMA の出荷時のデフォルト状態へのリセット (371 ページ)
- 技術サポートの有効化または無効化 (373 ページ)
- 主管理者の有効化または無効化 (376 ページ)
- キー配列の設定 (379 ページ)
- KMA からのログアウト (380 ページ)

セキュリティー責任者のメニューは次のとおりです。

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------
Please enter your User ID: SO
Please enter your Passphrase:

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on
glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------


(1)     Log KMA Back into Cluster
(2)     Set User's Passphrase
(3)     Set KMA Management IP Addresses
(4)     Set KMA Service IP Addresses
(5)     Modify Gateway Settings
(6)     Set DNS Settings
(7)     Reset to Factory Default State
(8)     Technical Support
(9)     Primary Administrator
(10)    Set Keyboard Layout
(0)     Logout
------------------------------------------------------------
Please enter your choice:
```

KMA のクラスタへの再ログイン

このメニューオプションを使用すると、セキュリティー責任者は、パスフレーズの変更後、KMA からクラスタにログインし直すことができます。

> **注 ー** 数時間以上にわたって KMA がクラスタからログアウトしている場合は、KMA を再度クラスタにログインさせる前に KMA をロックしてください。
>
> 「KMA List」パネルで「Replication Lag Size」に示されるように、最近の更新がこの KMA に伝播されてから、KMA をロック解除します。
>
> 詳細は、次の各項目を参照してください。
>
> - 222 ページの「Lock/Unlock KMA」
> - 119 ページの「「KMA List」メニュー」。

このタスクを実行するには、その前に次の処理を行う必要があります。

1. OKM Manager を起動します。
2. 既存の KMA にセキュリティー責任者としてログインします。
3. 「KMA List」パネルに移動します。
4. KMA エントリを作成します。

KMA からクラスタにログインするには、次の手順を実行します。

5. メインメニューの「`Please enter your choice:`」プロンプトで、**1** を入力して Enter キーを押します。次の情報が表示されます。

```
Log KMA Back into Cluster
------------------------------------------------------------
Press Ctrl-c to abort.
Please enter the Management Network IP Address of an existing
KMA in the cluster:

The KMA Passphrase is a Passphrase that you have
previously configured for this KMA to join a Cluster.

Please enter this KMA's Passphrase:
```

6. 既存の KMA (たとえば、129.80.60.172) にセキュリティー責任者としてログインします。

7. プロンプトで、KMA 用に最初に設定したパスフレーズを入力して Enter キーを押し、クラスタにログインします。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #1:

Please enter Key Split Passphrase #1:

Press Enter to continue:
```

8. OKM Manager の鍵分割資格変更機能で、はじめての KMA の QuickStart 中に設定した最初の鍵分割ユーザー名を入力します (216 ページの「鍵分割設定の変更」を参照)。

   注 ー セキュリティー責任者は、入力する鍵分割ユーザーの数、つまり鍵分割しきい値が何であるかを知っている必要があります。この例では、鍵分割しきい値は 2 です。

9. 鍵分割ユーザーのパスフレーズを入力して Enter キーを押します。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #2:

Please enter Key Split Passphrase #2:

Press Enter to continue:
```

10. 2 つめの鍵分割ユーザー名を入力します。

11. 鍵分割ユーザー用のパスフレーズを入力して、Enter キーを押します。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.

Press Ctrl-c to abort.
Please enter Key Split User Name #3:

Are you sure that you want to log the KMA back into the Cluster?
[y/n]: n

Press Enter to continue:
```

12. Key Split User Name #3 が表示されたら Enter キーを押して、鍵分割ユーザーの承認を終了します。

13. **n** を入力して Enter キーを押します。

ユーザーのパスフレーズの設定

このメニューオプションを使用すると、セキュリティー責任者は、セキュリティー責任者を含む任意のユーザーに対してパスフレーズを設定することができます。

ユーザーのパスフレーズを設定するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、**2** を入力して Enter キーを押します。次の情報が表示されます。

```
Set User's Passphrase
-------------------------------------------------------------
Press Ctrl-c to abort.
Please enter the User Name:
```

2. プロンプトで、ユーザー名を入力して Enter キーを押します。次の情報が表示されます。

```
Passphrases must be at least 8 characters and at most 64
characters in length.
Passphrases must not contain the User's User Name.
Passphrases must contain characters from 3 of 4 character
classes (uppercase, lowercase, numeric, other).

Please enter the desired Passphrase:

Please re-enter the desired Passphrase:

Press Enter to continue:
```

3. プロンプトで、パスフレーズを入力して Enter キーを押します。
4. 「Please re-enter the desired Passphrase:」プロンプトで、同じパスフレーズを入力して Enter キーを押します。次の情報が表示され、パスフレーズが設定されていることが示されます。

   ```
   Press Enter to continue:
   ```

   別のユーザーのパスフレーズを変更しようとした場合、次の情報が表示されます。

```
This command requires authorization by a quorum of Key
Split Users. Enter sufficient Key Split credentials to form
a quorum. Enter a blank name to finish.
-------------------------------------------------------------

Press Ctrl-c to abort.

Please enter Key Split User Name #1:
```

5. 最初の鍵分割ユーザー名を入力して Enter キーを押します。

```
Please enter Key Split Passphrase #1:

Press Enter to continue:
```

6. 最初の鍵分割パスフレーズを入力して Enter キーを押します。
7. 手順 5 と手順 6 を繰り返し、定足数を形成するために十分な数の鍵分割ユーザー名を入力します。
8. 「Key Split User Name」プロンプトが表示されたら Enter キーを押して、鍵分割ユーザーの承認を終了します。

   注 ー 十分な定足数の鍵分割資格を入力しない場合、ユーザーのパスフレーズの設定処理は保留中の定足数操作になります。詳細については、338 ページの「「Pending Quorum Operation List」メニュー」を参照してください。

9. Enter キーを押して、メインメニューに戻ります。

KMA の管理 IP アドレスの設定

このオプションは、KMA の管理アドレスの設定を変更します。この情報は、最初に QuickStart プログラムで設定され (51 ページの「ネットワーク構成の指定」を参照)、このオプションで変更することができます。

大規模なマルチサイトクラスタでは、ドライブがクラスタ内のすべての KMA のサブセットにのみ接続されている場合があります。次の注意事項は、ドライブを接続できる一連の KMA に適用されます。

> **注意 ー** この機能は、慎重に使用するようにしてください。ある KMA の情報を変更すると、その他のすべての KMA は、これらが接続されていれば、その更新をただちに受信します。KMA が接続されていない場合は、KMA がふたたび接続可能になると、その他の KMA を更新します。
>
> ただし、たとえば、ネットワーク異常により相互に接続していない 2 つの KMA が存在する場合に、両方の IP アドレスを変更すると、ネットワークが修復されてもそれらを再接続することはできません。
>
> この場合、一方の KMA に対して 360 ページの「KMA のクラスタへの再ログイン」の手順を使用してもう一方の KMA に再接続し、最初にパスフレーズを更新する必要があります。たとえば、KMA の A と B が接続されていない状態で両方の IP アドレスを変更した場合は、A にログインして B のパスフレーズを変更する必要があります。次に、B のコンソールにログインし、360 ページの「KMA のクラスタへの再ログイン」の手順を使用して A に再度接続します。
>
> テープドライブを使用する場合も注意してください。テープドライブは、更新された IP 情報を自動的に受信しません。テープドライブは、テープがマウントされるときにのみ、更新された IP 情報を取得します。このため、夜間にのみテープジョブを実行し、日中にすべての KMA の IP アドレスを変更する典型的な環境である場合、ドライブはどの KMA とも通信できません。この状況が発生した場合は、ドライブを OKM クラスタに再登録する必要があります。これを回避するために、KMA の IP アドレスを 1 つずつ変更し、すべてのドライブがその変更を受信するまで待機してから、次の変更を行なってください。

KMA の管理 IP アドレスを設定するには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**3** を入力して Enter キーを押します。

現在の KMA 管理 IP アドレスの設定が表示されます。IPv6 アドレスを使用するように KMA が設定されていない場合、IPv6 アドレスのフィールドは空白です。

```
Set KMA Management IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other KMAs or Users in your system.

Current settings:
  Management Configuration : Static
  Management IP Address    : 10.80.180.39
  Management Subnet Mask   : 255.255.254.0
  Management IPv6 Addresses: 2001:DB8::/32


Do you want to configure the Management Network interface to have
an IPv6 address? [y/n]:

Do you want to use DHCP to configure the Management Network
interface? [y/n]:

Please enter the Management Network IP Address [10.80.180.39]:

Please enter the Management Network Subnet Mask [255.255.254.0]:

Are you sure that you want to commit these changes? [y/n]: y
```

2. 「Do you want to configure the Management Network interface to have an IPv6 address」プロンプトで、**n** または **y** のいずれかを入力します。
3. 「Do you want to use DHCP to configure the Management Network interface」プロンプトで、**n** または y のいずれかを入力します。**n** を入力した場合は、手順 4 に進みます。**y** を入力した場合は、手順 6 に進みます。
4. プロンプトで、管理ネットワークの IP アドレスを入力して Enter キーを押します。
5. 「Please enter the Management Network Subnet Mask: 」プロンプトで、サブネットマスクアドレス (255.255.254.0 など) を入力して Enter キーを押します。
6. 「Are you sure that you want to commit these changes? [y/n]:」プロンプトで、**y** と入力します。

KMA のサービス IP アドレスの設定

このオプションは、KMA のサービスアドレスの設定を変更します。この情報は、最初に QuickStart プログラムで設定され (51 ページの「ネットワーク構成の指定」を参照)、このオプションで変更することができます。

大規模なマルチサイトクラスタでは、ドライブがクラスタ内のすべての KMA のサブセットにのみ接続されている場合があります。次の注意事項は、ドライブを接続できる一連の KMA に適用されます。

> **注意 ー** この機能は、慎重に使用するようにしてください。ある KMA の情報を変更すると、その他のすべての KMA は、これらが接続されていれば、その更新をただちに受信します。KMA が接続されていない場合は、KMA がふたたび接続可能になると、その他の KMA を更新します。
>
> ただし、たとえば、ネットワーク異常により相互に接続していない 2 つの KMA が存在する場合に、両方の IP アドレスを変更すると、ネットワークが修復されてもそれらを再接続することはできません。
>
> この場合、一方の KMA に対して 360 ページの「KMA のクラスタへの再ログイン」の手順を使用してもう一方の KMA に再接続し、最初にパスフレーズを更新する必要があります。たとえば、KMA の A と B が接続されていない状態で両方の IP アドレスを変更した場合は、A にログインして B のパスフレーズを変更する必要があります。次に、B のコンソールにログインし、360 ページの「KMA のクラスタへの再ログイン」の手順を使用して A に再度接続します。
>
> テープドライブを使用する場合も注意してください。テープドライブは、更新された IP 情報を自動的に受信しません。テープドライブは、テープがマウントされるときにのみ、更新された IP 情報を取得します。このため、夜間にのみテープジョブを実行し、日中にすべての KMA の IP アドレスを変更する典型的な環境である場合、ドライブはどの KMA とも通信できません。この状況が発生した場合は、ドライブを OKM クラスタに再登録する必要があります。これを回避するために、KMA の IP アドレスを 1 つずつ変更し、すべてのドライブがその変更を受信するまで待機してから、次の変更を行なってください。

現在の KMA サービス IP アドレスの設定が表示されます。IPv6 アドレスを使用するように KMA が設定されていない場合、IPv6 アドレスのフィールドは空白です。

```
Set KMA Service IP Addresses
------------------------------------------------------------

Press Ctrl-c to abort.

An IP Address configuration must be defined in order for the
KMA to communicate with other Agents in your system.

Current settings:
  Service Configuration : Static
  Service IP Address    : 192.168.1.39
  Service Subnet Mask   : 255.255.255.0
  Service IPv6 Addresses: 2001:DB8::/32


Do you want to configure the Service Network interface to have an
IPv6 address?
[y/n]:

Do you want to use DHCP to configure the Service Network interface?
[y/n]:

Please enter the Service Network IP Address [192.168.1.39]:

Please enter the Service Network Subnet Mask [255.255.255.0]:

Are you sure that you want to commit these changes? [y/n]: y
```

1. メインメニューの「`Please enter your choice:`」プロンプトで、**4** を入力して Enter キーを押します。
2. 「`Do you want to configure the Service Network interface to have an IPv6 address`」プロンプトで、**n** または **y** のいずれかを入力します。
3. 「`Do you want to use DHCP to configure the Service Network interface`」プロンプトで、**n** または y のいずれかを入力します。n を入力した場合は、手順 4 に進みます。**y** を入力した場合は、手順 6 に進みます。
4. プロンプトで、サービスネットワークの IP アドレスを入力して Enter キーを押します。
5. 「`Please enter the Service Network Subnet Mask:`」プロンプトで、サブネットマスクアドレス (255.255.255.0 など) を入力して Enter キーを押します。
6. 「`Are you sure that you want to commit these changes? [y/n]:`」プロンプトで、**y** と入力します。

ゲートウェイの表示、追加、削除

このメニューオプションでは、管理 (M) およびサービス (S) の各ネットワークインタフェースでの現在のゲートウェイ設定が 1 ページに 5 件ずつ表示され、ユーザーはゲートウェイの追加、ゲートウェイの削除、または現在のゲートウェイ構成の確認を実行できます。

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
   1 default                    10.80.181.254               0.0.0.0         M
   2 default                    10.80.181.21                0.0.0.0         M
   3 default                    192.168.1.119               0.0.0.0         S
   4 10.0.0.0                   10.80.180.25                255.255.254.0   M
*  5 10.80.180.0                10.80.180.39                255.255.254.0   M

Press Enter to continue:

Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                    Netmask         IF
---- -------------------------- -------------------------- --------------- --
*  6 192.168.1.0                192.168.1.39                255.255.255.0   S
   7 192.168.25.0               10.80.180.25                255.255.255.0   M
   8 192.168.26.0               10.80.180.25                255.255.255.0   M
*  9 127.0.0.1                  127.0.0.1                   255.255.255.255
* 10 fe80::                     fe80::216:36ff:feca:15b6    10              M

(1) Continue
(2) Back
1
```

```
Modify Gateway Settings
------------------------------------------------------------

Press Ctrl-c to abort.

Gateways that are configured automatically are not modifiable, and are
indicated with an asterisk (*). Management routes are indicated with an 'M',
and service routes with an 'S'.

   # Destination                Gateway                     Netmask         IF
---- -------------------------- -------------------------- --------------- --
* 11 fe80::                     fe80::216:36ff:feca:15b9    10              S

You can add a route, delete a route, or exit the gateway configuration.
Please choose one of the following:

(1)  Add a gateway
(2)  Remove a configured gateway (only if modifiable)
(3)  Exit gateway configuration
(4)  Display again
3
```

1. メインメニューの「`Please enter your choice:`」プロンプトで、**5** を入力して Enter キーを押します。
2. 「`(1)Continue (2)Back`」プロンプトで、次の 5 つのゲートウェイを表示するには **1** を、前の 5 つのゲートウェイを表示するには **2** を入力します。
3. 最後のゲートウェイが表示されたら、「`Please choose one of the following:`」プロンプトで **1**、**2**、**3**、または **4** を入力し、Enter キーを押します。

注 ー Ctrl+c を押すと常に、変更が保存されずにメインメニューに戻ります。

DNS 設定の指定

このメニューオプションでは、DNS 設定が表示され、ユーザーは新しい DNS ドメイン (DNS ドメインを構成する場合) および DNS サーバーの IP アドレスを指定できます。

```
Set DNS Configuration
------------------------------------------------------------

Press Ctrl-c to abort.

DNS configuration is optional, but necessary if this KMA
will be configured using hostnames instead of IP addresses.

Current DNS configuration:

Domain: central.sun.com
Nameservers: 10.80.0.5

Please enter the DNS Domain (blank to unconfigure DNS):
central.sun.com

Up to 3 DNS Name Servers can be entered. Enter each name
server separately, and enter a blank name to finish.

Please enter DNS Server IP Address #1: 10.80.0.5

Please enter DNS Server IP Address #2:
```

1. メインメニューの「`Please enter your choice:`」プロンプトで、**6** を入力して Enter キーを押します。
2. 「`Please enter the DNS Domain (blank to unconfigure DNS):`」プロンプトで、DNS ドメイン名を入力します。
3. 「`Please enter DNS Server IP address`」プロンプトで、DNS サーバーの IP アドレスを入力します。最大で 3 つの IP アドレスを入力できます。
4. IP アドレスを指定しないで終了するには、`Enter` キーを押します。

KMA の出荷時のデフォルトへのリセット

このメニューオプションを使用すると、セキュリティー責任者は、KMA を出荷時のデフォルト状態にリセットできます。

警告 ー リセットは回復不可能なため、KMA の情報は失われます。

これは破壊的な処理で、ハードディスクに格納されているすべてのデータが失われることになります。システムは強制的に再起動されます。ファイルシステムは再フォーマットされ、新しい暗号化鍵を使用するための準備が行われます。

KMA を出荷時のデフォルトにリセットするには、次の手順を実行します。

1. 「Please enter your choice:」プロンプトで、**7** を入力して Enter キーを押します。次の情報が表示されます。

```
Reset to Factory Default State
------------------------------------------------------------

Press Ctrl-c to abort.

WARNING:
All information stored on this KMA will be destroyed!
Access to all protected data will be lost unless a backup
of the KMA data has been created or Cluster Peer
KMAs are present.
Please consult the Administrative Guide before proceeding
with this operation.

The system will be rebooted after performing the reset.

Zeroize KMA before resetting (this process will take approximately
4 hours) [y/n]:

Are you sure that you want to reset the KMA to the
Factory Default State?

Type RESET to confirm: RESET

Press Enter to continue:
```

警告 ー この KMA のすべての情報は破壊されます。KMA のデータのバックアップが作成されているか、クラスタピア KMA が存在する場合を除き、すべての保護されたデータへのアクセスは失われます。

2. 「Zeroize KMA before resetting」プロンプトで、**n** または **y** のいずれかを入力します。**y** を入力した場合、ハードドライブのすべての情報が確実に完全消去されます。

   注 ー この処理には、約 4 時間かかります。

3. 「Type RESET to confirm」プロンプトで、**RESET** と入力して Enter キーを押します。次の情報が表示され、KMA のリセット中であることが示されます。

```
Resetting...
```

4. 認証が完了すると、QuickStart に戻ります。49 ページの「QuickStart プログラムの実行」を参照してください。

技術サポートアカウントの有効化

「Technical Support」メニューオプションを使用すると、オペレータはオペレーティングシステムのサポートアカウントとそのアカウントの SSH アクセスを有効または無効にすることができます。デフォルトでは、技術サポートアカウントおよび SSH アクセスはどちらも無効です。サポートアカウントのパスフレーズはオペレータが定義するため、サポートアカウントを有効にすると、OKM コンソールのユーザーには KMA への限定的なアクセス権が付与されます。

1. 技術サポートアカウントを有効にするには、次の手順を実行します。

メインメニューの「Please enter your choice:」プロンプトで、**8** を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが無効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently DISABLED.
************************ WARNING ***************************
Enabling the support account and SSH access is a SECURITY
RISK. These settings should not be left enabled unless required for
troubleshooting purposes.
Ensure that this account is disabled when not required.
************************************************************

Would you like to ENABLE the support account? [y/n]: y
```

2. 「Are you sure that you want to ENABLE the support account and assume this security risk? [y/n]」プロンプトで、**y** を入力して Enter キーを押し、アカウントを有効にします。SSH アクセスを使用可能にすると、技術サポートは遠隔から問題の診断を行うことができます。
3. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、SSH ホスト鍵の目的が示されます。

```
When a Technical Support representative connects to the
KMA using SSH, SSH host keys must be verified via an
alternative secure communication channel in order to detect
a potential "man-in-the-middle" attack.
Please record and store these SSH host keys securely.

SSH host keys are generated when SSH is enabled for the
first time. They may be subsequently regenerated to invalidate
the existing SSH host keys.
```

次の画面では、SSH 鍵を再生成するかどうかが確認され、サポートアカウントのパスフレーズの入力を求められます。

```
Would you like to regenerate the SSH host keys? [y/n]: y

A Passphrase for the support account must be at least 8
characters and at most 64 characters in length.

Please enter a Passphrase for the support account:

Please re-enter the Passphrase for the support account:

The maximum age of the Passphrase of the support account
is the maximum number of days that this Passphrase is valid.

When this age has been reached, then the support account
is disabled.

This number must be greater than 0.

Please enter the maximum age of this Passphrase: 2
```

4. 「Would you like to regenerate the SSH host keys?」プロンプトで、**y** を入力して Enter キーを押します。
5. 「Please enter a Passphrase for the support account:」プロンプトで、パスフレーズを入力します。

   注 ー パスフレーズの長さは、パスフレーズ最小長のセキュリティーパラメータの設定値以上である必要があります。この値は QuickStart プログラムの実行中に 8 に設定されますが、あとから OKM Manager の GUI で変更できます。211 ページの「セキュリティーパラメータの変更」を参照してください。
6. パスフレーズを再入力します。
7. パスフレーズの最長有効日数を入力します。
8. Enter キーを押して、メインメニューに戻ります。

```
Press Enter to continue:
```

技術サポートアカウントの無効化

注 ー このタスクの有効化はセキュリティー責任者のみが実行できます。無効化はオペレータまたはセキュリティー責任者が実行できます。

技術サポートアカウントを無効にするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**8** を入力して Enter キーを押します。次の情報が表示され、サポートアカウントが有効であることが示されます。

```
Technical Support
------------------------------------------------------------
Press Ctrl-c to abort.

The support account is currently ENABLED.

Would you like to DISABLE the support account? [y/n]: y
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE the support account? [y/
n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。SSH サービスは自動的に停止します。

主管理者の有効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

- 主管理者のアクセスを有効にするには、最初に技術サポートを有効にする必要があります (オプション 8)。
- このタスクの有効化はセキュリティー責任者のみが実行できます。無効化はオペレータまたはセキュリティー責任者が実行できます。

> **注意 ー** 主管理者機能を使用すると、ユーザーは、技術サポートとしてログインし、root によるアクセスと同等の主管理者のアクセスが許可されます。主管理者のパスフレーズを知っているのは Oracle サポートのみであるため、主管理者のアクセス権は Oracle サポートの担当者のみが取得できます。
>
> これは危険ですが、状況によっては、問題からシステムを回復させるために必要になる場合があります。ただし、バックラインサポートまたはエンジニアリングからの直接のガイダンスが必要なことがあります。

1. 主管理者のアクセスを有効にするには、次の手順を実行します。

メインメニューの「`Please enter your choice:`」プロンプトで、**9** を入力して Enter キーを押します。次の情報が表示され、主管理者のアクセスが無効であることが示されます。

```
Primary Administrator
------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently DISABLED.

************************* WARNING ************************
Providing the support account with Primary Administrator
privileges
is a SECURITY RISK. This setting should not be left enabled unless
required for troubleshooting purposes.

Ensure that these privileges are disabled when not required.
**********************************************************

Would you like to ENABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを有効にします。

3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to ENABLE these privileges for the
support account, assuming this security risk? [y/n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。主管理者のアクセスが有効になりました。

主管理者の無効化

「Primary Administrator」メニューオプションを使用すると、KMA に対する主管理者のアクセスを有効または無効にすることができます。

> **注 ー** このタスクの有効化はセキュリティー責任者のみが実行できます。無効化はオペレータまたはセキュリティー責任者が実行できます。

主管理者のアクセスの無効化は即時に実行されます。別のユーザーが主管理者として接続している場合、このアクセスを無効にすると、次に実行が試みられたコマンドは失敗します。

1. 主管理者のアクセスを無効にするには、次の手順を実行します。

メインメニューの「`Please enter your choice:`」プロンプトで、**9** を入力して Enter キーを押します。次の情報が表示され、アクセスが有効であることが示されます。

```
Primary Administrator
-------------------------------------------------------------

Press Ctrl-c to abort.

The Primary Administrator role is currently ENABLED.

Would you like to DISABLE Primary Administrator privileges for the
support account? [y/n]: y

Are you sure that you want to DISABLE these privileges for the
support account? [y/n]: y

Primary Administrator configuration changes have been completed.

Press Enter to continue:
```

2. プロンプトで、**y** を入力して Enter キーを押し、アカウントを無効にします。
3. 次の情報が表示され、変更の確認を求めるプロンプトが表示されます。

```
Are you sure that you want to DISABLE these privileges for the
support account? [y/n]:
```

4. プロンプトで、**y** を入力して Enter キーを押します。主管理者のアクセスが無効になりました。

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

> **注 ー** 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. 「Please enter your choice:」プロンプトで、**7** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian       ( 2) Belarusian    ( 3) Belgian
( 4) Bulgarian      ( 5) Croatian      ( 6) Danish
( 7) Dutch          ( 8) Finnish       ( 9) French
(10) German         (11) Icelandic     (12) Italian
(13) Japanese-type6 (14) Japanese      (15) Korean
(16) Malta_UK       (17) Malta_US      (18) Norwegian
(19) Portuguese     (20) Russian       (21) Serbia-And-Montenegro
(22) Slovenian      (23) Slovakian     (24) Spanish
(25) Swedish        (26) Swiss-French  (27) Swiss-German
(28) Taiwanese      (29) TurkishQ      (30) TurkishF
(31) UK-English     (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「Please enter the keyboard layout [US-English] :」プロンプトで、キー配列を変更する言語を入力します。
3. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、変更が行われたことが示されます。Enter キーを押して、メインメニューに戻ります。

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

ログアウト

現在の OKM コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、OKM コンソールにふたたびログインできます。

その他の役割の機能

この節では、その他の役割 (コンプライアンス責任者、バックアップオペレータ、監査者、定足数メンバー) が実行できる機能について説明します。次の機能があります。

- キー配列の設定 (382 ページ)
- KMA からのログアウト (383 ページ)

```
Oracle Key Manager Version 2.5 (Build1195.1)
------------------------------------------------------------

Oracle Key Manager Version 2.5 (Build1195.1) -- OP on
glenkinchiekma
SN: 0710QAL0CF
------------------------------------------------------------

(1)  Set Keyboard Layout
(0)  Logout

------------------------------------------------------------------
Please enter your choice:
```

キー配列の設定

このオプションを使用すると、キー配列を英語から各種言語に変更できます。

> **注 ー** 押したキーを KMA が正しく解釈するために、キー配列の設定が KMA に接続されたキーボードの配列と一致するようにしてください。

キー配列を設定するには、次の手順を実行します。

1. メインメニューの「Please enter your choice:」プロンプトで、**1** を入力して Enter キーを押します。次のようにキー配列が表示されます。

```
Set Keyboard Layout
-------------------------------------------------------------

Press Ctrl-c to abort.
You may change the keyboard layout here.

Available keyboard layouts:

( 1) Albanian       ( 2) Belarusian    ( 3) Belgian
( 4) Bulgarian      ( 5) Croatian      ( 6) Danish
( 7) Dutch          ( 8) Finnish       ( 9) French
(10) German         (11) Icelandic     (12) Italian
(13) Japanese-type6 (14) Japanese      (15) Korean
(16) Malta_UK       (17) Malta_US      (18) Norwegian
(19) Portuguese     (20) Russian       (21) Serbia-And-Montenegro
(22) Slovenian      (23) Slovakian     (24) Spanish
(25) Swedish        (26) Swiss-French  (27) Swiss-German
(28) Taiwanese      (29) TurkishQ      (30) TurkishF
(31) UK-English     (32) US-English


The current layout is US-English
Please enter the number for the keyboard layout :

The keyboard layout has been applied successfully.

Press Enter to continue:
```

2. 「Please enter the keyboard layout [US-English] :」プロンプトで、キー配列を変更する言語を入力します。
3. プロンプトで、**y** を入力して Enter キーを押します。次の情報が表示され、変更が行われたことが示されます。Enter キーを押して、メインメニューに戻ります。

```
The keyboard layout has been applied successfully.

Press Enter to continue:
```

ログアウト

現在の OKM コンソールセッションからログアウトするには、次の手順を実行します。

1. メインメニューの「`Please enter your choice:`」プロンプトで、**0** を入力して Enter キーを押します。
2. 現在のセッションが終了して、ログインプロンプトが表示されます。ユーザーは、このログインプロンプトを使用して、OKM コンソールにふたたびログインできます。

12

コマンド行ユーティリティー

この章では、コマンド行ユーティリティーについて説明します。これらのユーティリティーを使用すると、ユーザーは OKM Manager の GUI からではなくコマンド行から、バックアップの起動、鍵のエクスポート、鍵のインポート、およびデータユニットの一覧表示を実行できます。

次のコマンド行ユーティリティーが使用可能です。

- 386 ページの「OKM コマンド行ユーティリティー」
- 404 ページの「バックアップコマンド行ユーティリティー」。

注 – OKM コマンド行ユーティリティーは、バックアップコマンド行ユーティリティーに優先します。可能であれば常に、OKM コマンド行ユーティリティーを使用することをお勧めします。

OKM コマンド行ユーティリティー

OKM コマンド行ユーティリティーを使用すると、次を行うことができます。

- 自動バックアップのスケジュール設定
- OKM コアセキュリティーのバックアップ
- 鍵のインポートとエクスポート
- 鍵の破棄
- 監査イベントの一覧表示
- データユニットの一覧表示
- 複数のエージェントの作成または変更

バックアップコマンド行ユーティリティーと異なり、このユーティリティーではユーザー名とパスフレーズの代わりに X.509 証明書を使用して、ユーティリティー自体を有効な OKM ユーザーとして認証できます。そのため、ユーザーがコマンド行でパスフレーズを入力する必要はありません。

次の表で、これらの機能を実行できる役割について詳しく説明します。

表 12-1 OKM コマンド行ユーティリティー - ユーザーの役割アクセス

処理 :	Role:
バックアップ	バックアップオペレータ
OKM コアセキュリティーのバックアップ	セキュリティー責任者
鍵のインポート / エクスポート	オペレータ
鍵の破棄	オペレータ
監査イベントの一覧表示	すべての役割*
データユニットの一覧表示	オペレータ / コンプライアンス責任者
エージェントの作成	オペレータ
エージェントのデフォルト鍵グループの設定 / 変更	コンプライアンス責任者
エージェントのプロパティーの変更	オペレータ
エージェントの一覧表示	オペレータ / コンプライアンス責任者

*. エージェント ID、データユニット ID、または鍵 ID を指定する場合は、オペレータまたはコンプライアンス責任者の役割が必要です。

このユーティリティーは OKM Manager の GUI とともに、同じインストーラを使用してインストールされます。

注 ー リンクローカル IPv6 アドレスを入力する場合、OKM コマンド行ユーティリティーを起動し、リンクローカル IPv6 アドレスを指定します。「%4」などのゾーン ID をアドレスの末尾に含めるようにしてください。

初期設定時に従う必要がある手順については、114 ページの「ゾーン ID を含む IPv6 アドレス」を参照してください。

Solaris/Windows の構文

```
okm -v | --version | --help | -h
```

```
 okm backup [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                [ --directory=dirname ] ] | --oper=username
                [ --retries=retries ] [ --timeout=timeout ]
                [ --verbose=boolean ]
                  --kma=networkaddress
                  --output=dirname
```

```
 okm backupcs [ [ [ --cacert=filename ] [ --usercert=filename ]]
                  [ --directory=dirname ] | --oper=username ]
                  [ --retries=retries ] [ --timeout=timeout ]
                  [ --verbose=boolean ]
                    --kma=networkaddress
                    --output=filename
```

```
okm destroykeys [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                  [ --directory=dirname ] | --oper=username ]
                  [ --retries=retries ] [ --timeout=timeout ]
                  [ --verbose=boolean ]
                    --kma=networkaddress
                    --duids=filename | --all=true
                    --keystate=keystate
                    --comment="text"
```

```
 okm export [ [ [ --cacert=filename ] [ --usercert=filename ] ]
                [ --directory=dirname ] | --oper=username ]
                [ --retries=retries ] [ --timeout=timeout ]
                [ --listwait=waittime ] [ --verbose=boolean ]
                  --filter=filter | --duids=filename
                  --kma=networkaddress
                  --output=filename
                  --partner=transferpartnerid
```

```
okm import [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
               [ --retries=retries ] [ --timeout=timeout ]
               [ --verbose=boolean ]
                 --kma=networkaddress
                 --input=filename
                 --partner=transferpartnerid
                 --keygroup=keygroupid
```

```
okm listauditevents [ [ [ --cacert=filename ]
                          [ --usercert=filename ] ]
                          [ --directory=dirname ] |
                            --oper=username ]
                          [ --filter=filter ]
                          [ --localtimezone=boolean ]
[ --maxcount=count ]
[ --retries=retries ]
[ --timeout=timeout ]
[ --verbose=boolean ]
[ --output=filename ]
[ --agentids=agentids |
--dataunitids=dataunitds |
--keyids=keyids ]
--kma=networkaddress
```

```
okm listdu [ [ [ --cacert=filename ] [ --usercert=filename ] ]
               [ --directory=dirname ] ] | --oper=username
               [ --filter=filter ]
               [ --retries=retries ] [ --timeout=timeout ]
               [ --listwait=waittime ] [ --verbose=boolean ]
               [ --output=filename ]
                 --kma=networkaddress
```

```
okm createagent[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                   [ --directory=dirname ] | --oper=username ]
                   [ --retries=retries ] [ --timeout=timeout ]
                   [ --verbose=boolean ]
                   [ --description=description ]
                   [ --site=siteid ]
                   [ --keygroup=defaultkeygroupid ]
                   [ --onetimepassphrase=boolean ]
                     --kma=networkaddress
                     --agent=agentid
                     --passphrase=agentpassphrase
```

```
okm listagents[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                [ --directory=dirname ] | --oper=username ]
                [ --retries=retries ] [ --timeout=timeout ]
                [ --listwait=waittime ] [ --verbose=boolean ]
                [ --filter=filter ] [ --output=filename ]
                  --kma=networkaddress
```

```
okm modifyagent[ [ [ --cacert=filename ] [ --usercert=filename ] ]
                 [ --directory=dirname ] | --oper=username ]
                 [ --retries=retries ] [ --timeout=timeout ]
                 [ --verbose=boolean ]
                 [ --description=description ] |
                 [ --site=siteid ] |
                 [ --keygroup=defaultkeygroupid ] |
                 [ --passphrase=agentpassphrase ] |
                 [ --enabled=boolean ] |
                 [ --onetimepassphrase=boolean ]
                   --kma=networkaddress
                   --agent=agentid
```

パラメータの解説

サブコマンド

backup

backup サブコマンドは、OKM データのバックアップを生成し、このバックアップを、指定された出力ディレクトリ内のバックアップデータファイルおよびバックアップ鍵ファイルにダウンロードします。

backupcs

backupcs サブコマンドは、OKM コアセキュリティーのバックアップを生成し、このバックアップを出力ファイルに格納します。

destroykeys

destroykeys サブコマンドは、非アクティブ化または危殆化された鍵を破棄します。

export

export サブコマンドは、OKM を使用して確立された転送パートナー用の、セキュリティー保護された鍵ファイルを作成します。データユニットのリストと関連付けられるすべての鍵は、この鍵ファイルを使用してエクスポートされ、鍵ファイルに署名する AES 256 ビット鍵を使用して保護されます。このデータユニットのリストは、指定されたフィルタ文字列またはファイル名の結果です。その後、この鍵ファイルと import サブコマンドを使用して、転送パートナーの OKM に鍵をインポートできます。kms コマンドの 1 回の呼び出しで、最大 1,000 個のデータユニットをエクスポートできます。

import

import サブコマンドは、OKM を使用して確立された、転送パートナー用のセキュリティー保護された鍵ファイルを読み取ります。鍵とそれに関連付けられたデータユニットは、この鍵ファイルを使用してインポートされます。鍵ファイルの検証には、インポート側 OKM の鍵転送非公開鍵が使用されます。このファイルは、以前に export サブコマンドを使用して別の OKM からエクスポートされたものである必要があります。

listauditevents

listauditevents サブコマンドは、監査イベントを一覧表示します。

listdu

listdu サブコマンドは、データユニットとそのプロパティーを一覧表示します。export サブコマンドを実行する前にこのサブコマンドを呼び出すと、指定されたフィルタ (ある場合) を使用してエクスポートされるデータユニットを調べることができます。

オプション

次のオプション一覧では、オプションの省略名と完全名を示します。オプションの完全名と値は等号 (=) によって区切られます。オプションの省略名と値はスペースによって区切られます。

次のオプションはユーザー認証に使用されます。

> **注 ー** `--cacert`、`--directory`、および `--usercert` の各オプションを指定してこのユーティリティーを呼び出す前に、ユーザーはまず OKM Manager の GUI から、ルート認証局およびユーザーの X.509 証明書をエクスポートする必要があります。

--cacert=*filename*

省略名 : -a

このユーティリティーが OKM での認証に使用する、OKM ルート認証局の X.509 証明書の PEM ファイルを指定します。このオプションを指定しない場合、ユーティリティーは `--directory` オプションで指定されたディレクトリから ca.crt ファイルを探します。このオプションは `--oper` オプションと相互に排他的です。

--directory=*dirname*

省略名 : -d

OKM ルート認証局の X.509 証明書が格納された PEM ファイルと、OKM ユーザーの X.509 証明書が格納された PEM ファイルを検索するディレクトリを指定します。指定しない場合、このユーティリティーは現在の作業用ディレクトリから証明書ファイルを探します。このオプションは `--oper` オプションと相互に排他的です。

--oper=*username*

省略名 : -b

このユーティリティーが OKM での認証に使用する OKM ユーザー ID を指定します。このオプションを指定する場合、証明書は使用されないため、ユーザーのパスフレーズの入力を求められます。このオプションは `--cacert`、`--usercert`、および `--directory` の各オプションと相互に排他的です。

--usercert=*filename*

省略名 : -u

このユーティリティーが OKM での認証に使用する、OKM ユーザーの X.509 証明書の PEM ファイルを指定します。この証明書ファイルには、ユーザーの非公開鍵も格納されている必要があります。指定しない場合、ユーティリティーは `--directory` オプションで指定されたディレクトリから `clientkey.pem` ファイルを探します。このオプションは `--oper` オプションと相互に排他的です。

追加オプションの一覧を次に示します。

--agentids=*agentids*

省略名 : -A

関連付けられた監査イベントのエージェント ID のコンマ区切りリストを指定します。各エージェント ID は 1-64 文字でなければなりません。このオプションを指定するには、OKM ユーザーにオペレータまたはコンプライアンス責任者の役割が必要です。このオプションは `--dataunitids` および `--keyids` の各オプションと相互に排他的です。

--all=true

省略名 : -l

このユーティリティーがすべてのデータユニットを対象に、`--keystate` オプションの指示に従い、非アクティブ化または危殆化された鍵をすべて破棄することを指示します。このオプションは `--duids` オプションと相互に排他的です。

--comment=*"text"*

省略名 : -C

鍵の破棄を記述する注釈を指定します。この注釈は 1 - 64 文字でなければなりません。

--dataunitids=*dataunitds*

省略名 : -D

関連付けられた監査イベントのデータユニット ID のコンマ区切りリストを指定します。各データユニット ID は 32 文字の 16 進値でなければなりません。このオプションを指定するには、OKM ユーザーにオペレータまたはコンプライアンス責任者の役割が必要です。このオプションは `--agentids` および `--keyids` の各オプションと相互に排他的です。

--duids=*filename*

省略名 : -i

このオプションは、鍵のエクスポートまたは破棄処理用に、データユニット ID の集合を記述したファイル名を定義します。ID は 1 行に 1 つずつ記述され、改行で区切られます。各データユニット ID は 32 文字の 16 進値でなければなりません。`destroykeys` サブコマンドで、非アクティブ化または危殆化された鍵が特定のデータユニットに存在しない場合、そのデータユニットは無視されます。指定されたファイルが空の場合、`destroykeys` サブコマンドはすべてのデータユニットを対象に、非アクティブ化または危殆化されたすべてのファイルを破棄します (`--all` オプションを参照)。このオプションは、`--filter` および `--all` の各オプションと相互に排他的です。

--filter=*filter*

省略名 : -f

表示またはエクスポートするデータユニット ID のリスト、または表示する監査イベントのリストを生成するために処理されるフィルタ文字列を指定します。文字列に空白が含まれる場合、文字列を引用符 (Windows では二重引用符) で囲む必要があります (397 ページの「例」を参照)。

> **注 ー** エクスポートにかかる時間はデータユニットと鍵の数に比例するため、通常は、データユニットの集合を縮小するフィルタを指定することをお勧めします。

export サブコマンドでは、このオプションは `--duids` オプションと相互に排他的です。

`export` および `listdu` サブコマンドでは、このフィルタ文字列の構文は次のとおりです。

```
DUState=state[, Exported=boolean ][, Imported=boolean]
[, DataUnitID=duid][, ExternalTag=tag][,
ExternalUniqueID=euid]
```

`DUState=`*`state`*
`state` に指定できる値は「normal」、「needs-rekey」、または「normal+needs-rekey」です。`DUState` フィルタを指定しない場合のデフォルトは「DUState=normal+needs-rekey」です。

`Exported=`*`boolean`*
`boolean` に指定できる値は「true」または「false」です。`Exported` フィルタ条件を指定しない場合、データユニットの選択時にエクスポート状態は考慮されないため、エクスポート済みデータユニットとまだエクスポートされていないデータユニットの両方が選択可能です。

`Imported=`*`boolean`*
`boolean` に指定できる値は「true」または「false」です。`Imported` フィルタ条件を指定しない場合、データユニットの選択時にインポート状態は考慮されないため、インポート済みデータユニットとまだインポートされていないデータユニットの両方が選択可能です。

`DataUnitID=`*`duid`*
`duid` はデータユニット ID です。

`ExternalTag=`*`tag`*
`tag` は外部タグです (LTO テープドライブ用に作成されるデータユニットの場合、スペースを使用してタグを 32 文字にパディングする必要があります)。

ExternalUniqueID=*euid*
euid は外部一意 ID です。

listauditevents サブコマンドでは、このフィルタ文字列の構文は次のとおりです。

```
StartDate=date[, EndDate=date ][, Severity=text]
[, Operation=text][, Condition=text] [, Class=text]
[, RetentionTerm=text] [, KMAName=kmaname]
[, EntityID=entityid][, EntityNetworkAddress=netaddress]
[, SortOrder=order][, ShowShortTerm=boolean]
```

StartDate=*date*
date の形式は *YYYY-MM-DD hh*:*mm*:*ss* で、これは UTC 時間を表します。

EndDate=*date*
date の形式は *YYYY-MM-DD hh*:*mm*:*ss* で、これは UTC 時間を表します。

Severity=*text*
text は監査重要度文字列です (例 : 「Error」)。

Operation=*text*
text は監査操作文字列です (例 : 「Retrieve Root CA Certificate」)。

Condition=*text*
text は監査条件文字列です (例 : 「Success」)。

Class=*text*
text は監査クラス文字列です (例 : 「Security Violation」)。

RetentionTerm=*text*
text は監査保持期間文字列です (例 : 「MEDIUM TERM RETENTION」)。

KMAName=*kmaname*
kmaname は KMA 名です。

EntityID=*entityid*
entityid は実体 ID です。

EntityNetworkAddress=*netaddress*
netaddress は IP アドレスまたはホスト名です。

SortOrder=*order*
order に指定できる値は「asc」または「desc」です。デフォルトでは、監査イベントは作成日の降順で表示されます。

ShowShortTerm=*boolean*
boolean に指定できる値は「true」または「false」です。デフォルトでは、保持期間が短期の監査イベントは表示されません。

--help

省略名 : -h

ヘルプ情報を表示します。

--input=*filename*

省略名 : -i

データユニットおよび鍵のインポート元のファイル名を指定します。このファイルは鍵転送ファイルとも呼ばれます。

--keygroup=*keygroupid*

省略名 : -g

OKM に対して定義される鍵グループの ID を指定します。

--keyids=*keyids*

省略名 : -K

関連付けられた監査イベントの鍵 ID のコンマ区切りリストを指定します。このオプションを指定するには、OKM ユーザーにオペレータまたはコンプライアンス責任者の役割が必要です。このオプションは、--agentids および --dataunitids の各オプションと相互に排他的です。

--keystate=*keystate*

省略名 : -s

破棄する鍵の状態を指定します。keystate に指定できる値は、非アクティブ化された鍵を指定する「deact」、危殆化された鍵を指定する「comp」、非アクティブ化または危殆化された鍵を指定する「deact+comp」のいずれかです。

--kma=*networkaddress*

省略名 : -k

要求を実行する KMA のネットワークアドレスを指定します。ネットワークアドレスはホスト名、IPv4 アドレス、または IPv6 アドレスで指定できます。

--listwait=*waittime*

省略名 : -w

export および listdu サブコマンドによって実行されるデータユニット一覧表示要求の間隔を秒数で指定します。デフォルト値は 2 です。

--localtimezone=*boolean*

省略名 : -L

監査イベントのタイムスタンプを、協定世界時 (UTC) ではなくローカルタイムゾーンで表示します。また、StartDate および EndDate の各フィルタがローカル時刻に解釈されるようにします。

--maxcount=*count*

省略名 : -c

一覧表示する監査イベントの最大数を指定します。デフォルト値は 20,000 です。

--output=*filename* or ***dirname***

省略名 : -o

結果が格納されるファイルの名前を指定します。これらの結果は、`backup` および `backupcs` 要求の場合はバックアップ、`export` 要求の場合は鍵転送ファイル、`listdu` 要求の場合はデータユニットとそのプロパティーの一覧表示、`listauditevents` 要求の場合は監査イベントの一覧表示です。`listdu` および `listauditevents` 要求の場合、`stdout` を表す「-」を指定でき、これはデフォルト値でもあります。`backup` 要求の場合、このオプションは、バックアップデータファイルとバックアップ鍵ファイルがダウンロードされるディレクトリを指定します。

--partner=*transferpartnerid*

省略名 : -p

OKM に対して定義され、エクスポートされた鍵を送信または受信する資格を持つ転送パートナーの ID を指定します。

--retries=*retries*

省略名 : -r

KMA がビジー状態の場合に、このユーティリティーが KMA への接続を試行する回数を指定します。デフォルト値は 60 です。

--timeout=*timeout*

省略名 : -t

これらの再試行間のタイムアウト値を秒単位で指定します。デフォルト値は 60 です。

--verbose=*boolean*

省略名 : -n

要求の処理の間、進捗状態を含む詳細出力をこのユーティリティーが生成することを指示します。boolean に指定できる値は「true」または「false」です。

--version

省略名 : -v

コマンド行の使用法を表示します。

例

これらの例では単一のコマンド行を示します。読みやすさのために、複数行に分けてコマンド行を示している場合があります。Solaris の例では、バックスラッシュはコマンド行の続きを示します。

次の例は、指定されたディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用してバックアップを生成します。

Solaris:

```
okm backup --kma=mykma1 \
           --directory/export/home/Joe/.sunw/kms/BackupOperatorCertificates \
           --output=/export/home/KMSBackups
```

Windows:

```
okm backup --kma=mykma1
           --directory=D:\KMS\Joe\BackupOperatorCertificates
           --output=D:\KMS\KMSBackups
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用してバックアップを生成します。

Solaris:

```
okm backup -k mykma1 -o /export/home/KMSBackups -b Joe
```

Windows:

```
okm backup -k mykma1 -o D:\KMS\KMSBackups -b Joe
```

次の例は、現在の作業用ディレクトリ内の ca.pem および op.pem ファイルの証明書を認証に使用して鍵をエクスポートします。

Solaris:

```
okm export -k 10.80.88.88 -d "." -a ca.pem -u op.pem \
           -f "DUState = normal+needs-rekey, Exported = false" \
           -o Partner.dat -p Partner
```

Windows:

```
okm export -k 10.80.88.88 -d "." -a ca.pem -u op.pem
           -f "DUState = normal+needs-rekey, Exported = false"
           -o Partner.dat -p Partner
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用して鍵をエクスポートします。

Solaris:

```
okm export --kma=mykma1 --oper=tpFreddy \
           --filter="Exported = false" --output=Partner.dat \
           --partner=Partner
```

Windows:

```
okm export --kma=mykma1 --oper=tpFreddy
           --filter="Exported = false" --output=Partner.dat
           --partner=Partner
```

次の例は、現在の作業用ディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用して鍵をインポートします。

Solaris:

```
okm import --kma=10.80.88.88 --directory="." \
           --input=DRKeys.dat --partner=Partner \
           --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
okm import --kma=10.80.88.88 --directory="."
           --input=DRKeys.dat --partner=Partner
           --keygroup=OpenSysBackupKeyGroup
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用して鍵をインポートします。

Solaris:

```
okm import --kma=mykma1 --oper=Joe --input=DRKeys.dat \
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

Windows:

```
okm import --kma=mykma1 --oper=Joe --input=DRKeys.dat
           --partner=Partner --keygroup=OpenSysBackupKeyGroup
```

次の例は、指定されたディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用してデータユニットを一覧表示します。

Solaris:

```
okm listdu --kma=10.80.88.88 \
           --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
           --output=/export/home/KMSDataUnits
```

Windows:

```
okm listdu --kma=10.80.88.88
           --directory=D:\KMS\Joe\OperatorCertificates
           --output=D:\KMS\KMSDataUnits
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用してデータユニットを一覧表示します。

Solaris:

```
okm listdu -k mykma1 -b Joe -f "Exported=false" \
           --output=/export/home/KMSDataUnits
```

Windows:

```
okm listdu -k mykma1 -b Joe -f "Exported=false"
           --output=D:\KMS\KMSDataUnits
```

次の例は、指定されたディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用して監査イベントを一覧表示します。

Solaris:

```
okm listauditevents --kma=10.80.88.88 \
              --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                   --filter=Severity=Error \
                   --output=/export/home/KMSAuditEvents
```

Windows:

```
okm listauditevents --kma=10.80.88.88
                    --directory=D:\KMS\Joe\OperatorCertificates
 --filter=Severity=Error
 --output=D:\KMS\KMSAuditEvents
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用して監査イベントを一覧表示します。

Solaris:

```
okm listauditevents -k mykma1 -b Joe -f "Severity=Error" \
                    --output=/export/home/KMSAuditEvents
```

Windows:

```
okm listauditevents -k mykma1 -b Joe -f "Severity=Error"
                    --output=D:\KMS\KMSAuditEvents
```

次の例は、指定されたディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用して、危殆化された鍵をすべて破棄します。

Solaris:

```
okm destroykeys --kma=10.80.88.88 \
                --directory=/export/home/Joe/.sunw/kms/OperatorCertificates \
                --all=true --keystate=comp \
                --comment="Joe destroyed compromised keys"
```

Windows:

```
okm destroykeys --kma=10.80.88.88
                --directory=D:\KMS\Joe\OperatorCertificates
                --all=true --keystate=comp
                --comment="Joe destroyed compromised keys"
```

次の例は、データユニット ID のリストと関連付けられた、非アクティブ化された鍵を破棄します。OKM ユーザーのユーザー ID とパスフレーズを認証に使用します。

Solaris:

```
okm destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt \
                -s deact -C "Joe destroyed deactivated keys"
```

Windows:

```
okm destroykeys -k mykma1 -b Joe -i DeactivatedDUIDs.txt
                -s deact -C "Joe destroyed deactivated keys"
```

次の例は、指定されたディレクトリ内の ca.crt および clientkey.pem ファイルの証明書を認証に使用してコアセキュリティーをバックアップします。

Solaris:

```
okm backupcs --kma=10.80.88.88 \
             --directory=/export/home/Joe/.sunw/kms/SecurityOfficerCertificates \
 --output=/export/home/KMSCoreSecurity.xml
```

Windows:

```
okm backupcs --kma=10.80.88.88
             --directory=D:\KMS\Joe\SecurityOfficerCertificates
             --output=D:\KMS\KMSCoreSecurity.xml
```

次の例は、OKM ユーザーのユーザー ID とパスフレーズを認証に使用してコアセキュリティーをバックアップします。

Solaris:

```
okm backupcs -k mykma1 -b Joe -o /export/home/KMSCoreSecurity.xml
```

Windows:

```
okm backupcs -k mykma1 -b Joe -o D:\KMS\KMSCoreSecurity.xml
```

終了値

次の終了値が返されます。

```
 0    Successful completion
 >0   An error occurred
```

サンプル Perl スクリプト

次に示すいくつかの基本的な Perl スクリプトは、カスタマイズして Solaris または Windows で実行できます。これらの例はすべて証明書ベースの認証を使用するため、実行するには、ルート認証局の証明書とユーザーの証明書が現在の作業用ディレクトリに置かれている必要があります。

> **注 ー** Perl スクリプトは OKM コマンド行ユーティリティーとともにインストールされません。Perl スクリプトから OKM コマンド行ユーティリティーを呼び出す場合は、テキストエディタを使用して、次のいずれかの Perl スクリプトと同様のスクリプトを作成します。

- `listdu.pl`

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.somewhere.com";
$FILTER="--filter=Exported=false";
$DIRECTORY=".";
$OUTPUT="listdu.txt";
system("$cmd listdu --verbose=true --directory=$DIRECTORY --kma=$KMA $FILTER
      --output=$OUTPUT")
```

- `export.pl`

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.somewhere.com";
$TP="DestinationPartner";
$FILTER="Exported=false";
$OUTPUT="$TP.dat";
system("$cmd export --verbose=true --kma=$KMA --directory=. --filter=$FILTER
      --partner=$TP --output=$OUTPUT");
```

- import.pl

```
#!/opt/csw/bin/perl
## the kms CLI utility must be in your path
$cmd="okm";
$KMA="kma1.somewhere.com";
$TP="SourceTransferPartner";
$KEYGROUP="MyKeyGroup";
$INPUT="../aberfeldy/KeyBundle.dat";
system("$cmd import --verbose=true --kma=$KMA --directory=. --partner=$TP
      --keygroup=$KEYGROUP --input=$INPUT");
```

- backup.pl

```
#!/opt/csw/bin/perl
## the following must be in your path
$cmd="okm";
$KMA="kma1.somewhere.com";
$DIRECTORY=".";
$OUTPUT=".";
system("$cmd backup --verbose=true --directory=$DIRECTORY --kma=$KMA
      --output=$OUTPUT")
```

バックアップコマンド行ユーティリティー

バックアップコマンド行ユーティリティーを使用すると、「Backup List」メニューからではなくコマンド行からバックアップを起動できます。自動バックアップのスケジュールを設定することもできます。

このユーティリティーは OKM Manager の GUI とともに、同じインストーラを使用してインストールされます。

> **注 –** リンクローカル IPv6 アドレスを入力する場合、バックアップユーティリティーを起動し、リンクローカル IPv6 アドレスを指定します。「%4」などのゾーン ID をアドレスの末尾に含めるようにしてください。
>
> 初期設定時に従う必要がある手順については、114 ページの「ゾーン ID を含む IPv6 アドレス」を参照してください。

Solaris の構文

```
OKM_Backup [-UserID userid] [-Passphrase passphrase]
           -KMAIPAddress IPaddress -BackupFilePath pathname
           [-Retries retries] [-Timeout timeout]
```

Windows の構文

```
OKMBackupUtility [-UserID userid] [-Passphrase passphrase]
                 -KMAIPAddress IPaddress -BackupFilePath pathname
                 [-Retries retries] [-Timeout timeout]
```

パラメータの解説

userid

バックアップオペレータのユーザー ID。これは Backup Operator である必要があります。

passphrase

ユーザー ID のパスフレーズ。

> **注 –** userid または passphrase の値が指定されない場合、ユーティリティーはこれらの値の入力を求めます。

IPaddress

バックアップを起動する場所となる KMA 管理ネットワークのアドレス。

pathname

バックアップファイルおよびバックアップ鍵ファイルがダウンロードされるシステム上の場所。

retries

KMA がビジー状態の場合に、このユーティリティーが KMA への接続を試行する回数。デフォルトは 60 です。

timeout

これらのエントリ間のタイムアウト値 (秒単位)。デフォルトは 60 です。

例

次の例は、バックアップファイル (形式 : OKM-Backup-backupid-timestamp.dat) およびバックアップ鍵ファイル (形式 : OKM-BackupKey-backupid-timestamp.xml) を作成します。

```
OKM_Backup -UserID MyBackupOperator -Passphrase secret2Me \
           -KMAIPAddress 129.80.60.172 \
           -BackupFilePath /tmp/MyKMSDownloads
```

A

SNMP 管理情報ベース (MIB) データ

この付録では、ネットワークで SNMP エージェントを構成し、OKM Manager の GUI で SNMP マネージャーを定義したユーザーを対象に、SNMP 情報について解説します。OKM Manager の GUI で 1 つ以上の SNMP マネージャーを定義すると、KMA がその SNMP マネージャーの IP アドレスに SNMP インフォームを送信します。

KMA はオブジェクト識別子 (OID) を使用して、次の情報を送信します。

表 A-2 KMA オブジェクト識別子

OID 値	種別	説明
1.3.6.1.4.1.42.2.22.99	----	汎用トラップ
1.3.6.1.4.1.42.2.22.99.1	列	日付 / 時刻
1.3.6.1.4.1.42.2.22.99.2	列	監査イベントクラス
1.3.6.1.4.1.42.2.22.99.3	列	監査イベント操作
1.3.6.1.4.1.42.2.22.99.4	列	監査イベント条件
1.3.6.1.4.1.42.2.22.99.5	列	Entity ID
1.3.6.1.4.1.42.2.22.99.6	列	ネットワークアドレス
1.3.6.1.4.1.42.2.22.99.7	列	メッセージ

SNMP マネージャーの表示、作成、および変更については、160 ページの「「SNMP Manager List」メニュー」を参照してください。

B

OKM を Advanced Security の Transparent Data Encryption (TDE) とともに使用する

この付録では、機密性のあるデータベース情報の暗号化または復号化を管理するために、Transparent Data Encryption (TDE) とともに OKM を使用することについて説明します。このソリューションでは、Oracle StorageTek テープドライブで使用されているのと同じ暗号化テクノロジーを使用して、Oracle データベースの暗号化鍵を管理できます。

Oracle Database 11gR2 の機能である Transparent Data Encryption は、次に対してデータベースの暗号化および復号化のサービスを提供します :

- Oracle Database 製品
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

この付録では、TDE に精通していることを想定しています。次の URL から入手できるドキュメント『Oracle Advanced Security Transparent Data Encryption Best Practices』を参照してください。

http://www.oracle.com/us/products/database/twp-transparent-data-encryption-bes-130696.pdf

Transparent Data Encryption (TDE) の概要

次の図は、Oracle データベースと Transparent Data Encryption (TDE) を利用した OKM クラスタを示しています。OKM クラスタの基本コンポーネントについては、第 1 章「紹介」を参照してください。

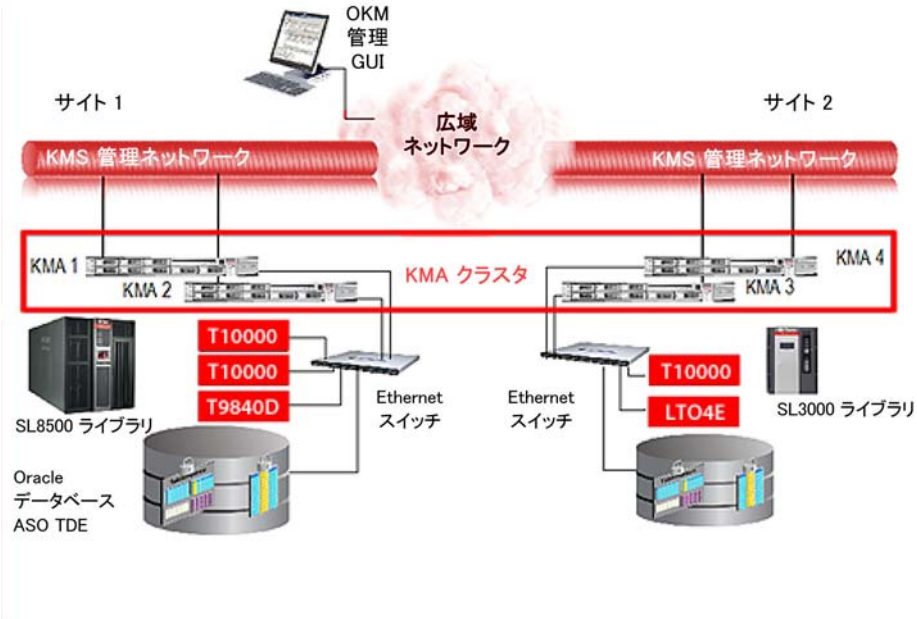


図 B-1 TDE を使用した OKM クラスタ

TDE は、TDE 列の暗号化およびテーブル領域の暗号化に、2 層鍵アプローチを使用した暗号化サービスを提供します。マスター暗号化鍵は、第 1 層で使用され、データベース内に格納されている第 2 層のテーブルまたはテーブル領域のデータ暗号化鍵を暗号化します。

TDE は、マスター暗号化鍵を外部のセキュリティーモジュール (Oracle Wallet または HSM) に格納します。これは、セキュリティーの実践として推奨されており、さまざまな脅威に対してもっとも高いレベルのセキュリティーを維持するために重要です。TDE のマスター暗号化鍵を安全に格納するために OKM を使用することは推奨されるアプローチです。

TDE で OKM を使用するように構成すると、OKM は AES256 マスター暗号化鍵を作成し、安全に保護します。OKM は、レプリケーション (クラスタ内の複数のコピー) および OKM 自体のバックアップにより鍵を保護します。

障害回復計画については、『OKM Disaster Recovery Guide』を参照してください。

OKM の PKCS#11 プロバイダ

PKCS#11 プロバイダは、Oracle Solaris および Oracle Enterprise Linux (OEL) で利用可能であり、TDE が OKM と連動することが保証されています。このプロバイダは、「pkcs11_kms」と呼ばれます。TDE は、組み込みでサポートされている Hardware Security Module (HSM) を使用して pkcs11_kms プロバイダを利用するように構成できます。

- Solaris の場合、pkcs11_kms プロバイダは、Solaris 暗号化フレームワークの構成可能なコンポーネントであり、PKCS#11 プロバイダ (cryptoadm (1M) を参照) を管理するための標準の Oracle Solaris サービスに準拠しています。
- Oracle Enterprise Linux (OEL) の場合は、pkcs11_kms プロバイダを個別にインストールしてから、Oracle Database で使用するために構成します。

pkcs11_kms プロバイダは、鍵の作成操作および鍵の取得操作のために OKM と対話します。暗号化および復号化の機能は、OKM ではなく、データベースで実行されます。

TDE などの PKCS#11 コンシューマアプリケーションは、それらが定義するラベルを使用して鍵オブジェクトを識別します。TDE は、マスター鍵が作成されたときにこのラベルを生成します。pkcs11_kms プロバイダは、このラベルを OKM に渡し、そこでデータユニットのメタデータとして維持管理されます。OKM では、鍵はデータユニットと関連付けられ、pkcs11_kms プロバイダの場合、この関係は常に 1 対 1 です。新しいマスター鍵が作成されるたびに、対応する鍵オブジェクトとともに鍵ラベルを持つデータユニットが作成されます。

詳細については、424 ページの「OKM 内の TDE マスター鍵の検出」を参照してください。

OKM での TDE の認証

管理ユーザーのログイン、鍵素材を取得するテープドライブ、または Oracle TDE などの PKCS#11 コンシューマのいずれであっても、OKM と対話するすべてのエンティティーは認証する必要があります。

TDE は、pkcs11_kms プロバイダを利用するために構成された特定のトークンを使用して OKM で認証します。このトークンは、セッションの各パーティー (具体的には、Oracle データベースインスタンスおよび OKM クラスタノード) の相互認証のためにパスワードベースの認証および X.509 証明書を使用します。これらの資格を PKCS#11 に適切に渡すように TDE を構成する必要があります。

構成の手順については、この付録の最初に参照したドキュメント『Oracle Advanced Security Transparent Data Encryption Best Practices』を参照してください。

認証資格の管理

OKM では、pkcs11_kms プロバイダを使用してエージェントの認証資格を管理できます。ポリシーの規定に応じて、エージェントのパスフレーズのリセット、およびエージェントの有効化、無効化、または削除を行うことができます。

セキュリティー違反が検出された場合、鍵の取得が拒否されるように特定のエージェントを無効化し、同時に、ほかのアプリケーションまたはデバイスにサービスを提供するほかのエージェントのアクセスは維持できます。

エージェントのパスフレーズをリセットする場合は、kmscfg (1M) ユーティリティーを再実行できます。このユーティリティーは、以前の構成を上書きする前に確認を求めます。

> **注意 ー** このプロファイルに格納されているメタデータが失われます (たとえば、ユーザーの PKCS#11 鍵ラベルのリスト)。そのトークンが鍵ラベルの生成のためにまだ使用されていない場合は、古いプロファイルを上書きしても安全です。

負荷分散とフェイルオーバー

pkcs11_kms プロバイダは、OKM クラスタサービス、ロードバランサ、およびクラスタのフェイルオーバーロジックを使用して OKM クラスタを認識します。KMS エージェントのコンポーネントは、クラスタ発見操作を定期的に発行することにより、OKM クラスタに対するクライアント側の認識を透過的に維持します。ネットワークの変更および OKM クラスタまたは KMA の可用性の変更は、pkcs11_kms プロバイダおよび TDE に代わって、エージェントが処理します。PKCS#11 の鍵生成および鍵取得の操作は、OKM クラスタの KMA 間で負荷分散されます。

鍵取得のパフォーマンスをさらに最適化するために、OKM サイトを使用してエージェントが KMA に関連付けられるように構成できます。この機能を使用すると、ネットワークトポロジに応じてサイトを定義できます。通常、サイト内の KMA およびエージェントは、WAN を経由するメンバー KMA およびエージェントと比べて、ネットワークの待ち時間が短くなります。

ネットワークセグメントまたは KMA が利用できない場合は、エージェント内のフェイルオーバーロジックによって、別の KMA が選択されて操作が完了します。TDE ではフェイルオーバーが認識されないため、鍵管理操作は非常に信頼性が高くなります。フェイルオーバーでは、同じサイト内の KMA がエージェントとして優先されます。

kmscfg (1M) ユーティリティーを使用すると、発見の頻度およびエージェントのフェイルオーバープロパティーを調整できます。

計画に関する考慮事項

Oracle Database に関する考慮事項

OKM は次のすべての Oracle Database 構成と互換性があります。

- 単一インスタンス、Oracle RAC One Node
- Oracle Database High Availability アーキテクチャー
  - Oracle RAC

    Oracle Database と Oracle Real Application Clusters (RAC) の組み合わせは OKM を使用できることが保証されています。Oracle RAC システムの各ノードには、TDE が使用する構成済みの pkcs11_kms プロバイダがある必要があります。すべてのノードは、認証用に同じ OKM エージェント ID を共有する必要があります。Oracle RAC では、ネットワークトポロジとして、パブリックおよびプライベートネットワークを利用します。Oracle RAC のノード間トラフィックに使用されるプライベートネットワークは、鍵取得トラフィックをより良く分離するために OKM のサービスネットワークと共有できます。このプライベートネットワークの構成方法によっては、これにより、プライベートネットワークの外部の KMA (リモートサイトの KMA など) へのエージェントのフェイルオーバーが妨げられる可能性があります。

    Oracle RAC の共有ストレージ要件および pkcs11_kms プロバイダの構成ファイルについては、419 ページの「pkcs11_kms のインストールおよび構成」を参照してください。
  - Oracle RAC Extended Cluster

    この構成では、取得時間を最小化するために、OKM クラスタ内の KMA を Oracle RAC ノードと同じネットワークに配置する必要があります。
  - Oracle Exadata Database Machine

    前述した「Oracle RAC」を参照してください。
- Oracle Data Guard

  すべてのセカンダリデータベースは、プライマリデータベースによって使用されるのと同じ OKM クラスタにアクセスします。
- 複数のデータベースインスタンス

  1 つのホスト上で複数の独立したデータベースインスタンスを実行する場合は、各インスタンスに PKCS#11 トークンを構成する必要があります。そのため、各データベースインスタンスに対して OKM エージェントを作成し、OKM へのエージェントの認証をトークンを使用して行います。このタスクを実行するには、kmscfg (1M) ツールを使用します。

  同じホスト上での複数のデータベースの実行については、この付録の最初に参照したドキュメント『Oracle Advanced Security Transparent Data Encryption Best Practices』を参照してください。
- Oracle RMAN

- Oracle Data Pump

OKM のパフォーマンスおよび可用性に関する考慮事項

pkcs11_kms トークンを使用した TDE の鍵取得は、通常、1 回の KMA アクセスで 100 - 200 ミリ秒かかります。フェイルオーバーが発生すると、応答時間はフェイルオーバーの試行回数を乗算した時間になります。

OKM のバックアップ操作および鍵転送操作は、リソースに負荷がかかるアクティビティーであり、OKM データベースのパフォーマンスに影響する場合があります。OKM のバックアップを行うタイミングと対象を十分に計画して決定してください。

OKM のバックアップは、クラスタ全体で行われるため、Oracle Database インスタンスで使用されていない KMA で実行できます。同様に、鍵転送操作もクラスタ全体の操作であり、任意の KMA で実行できます。このため、使用中の Oracle Database インスタンスで利用されていない KMA を選択することを推奨します。

障害回復の計画

OKM の障害回復計画については、『OKM Disaster Recovery Guide』および Oracle データベースの出版物を参照してください。

障害回復計画での決定事項は、ネットワーク計画の立案に影響します。pkcs11 プロバイダの設定ディレクトリは、障害回復計画の新しい考慮事項です。pkcs11_kms トークンを再構成する必要がないように (特に Oracle RAC のノード間で共有される場合)、この記憶領域の回復シナリオを検討します。

ネットワークの計画

OKM のクラスタ構成は、Oracle Database サーバーおよび企業の障害回復方針に従って計画する必要があります。OKM のネットワークオプションは、非常に柔軟であり、OKM の管理およびサービスネットワークで使用されるマルチホームのインタフェースが含まれています。詳細は、『Oracle Key Manager システムアシュアランスガイド』を参照してください。

鍵管理の計画

鍵管理の計画では、企業の鍵のライフサイクルおよびセキュリティーポリシーを検討する必要があります。これらの考慮事項によって、必然的にデータ保持について検討することになります。

- NIST SP-800 の鍵管理フェーズおよび対応する OKM の鍵の状態については、21 ページの「状態遷移」を参照してください。
- 421 ページの「OKM ポリシーベースの鍵の期限切れによる鍵の再作成」を参照してください。

鍵ポリシーに関する考慮事項

すべての TDE マスター鍵は、AES 256 ビットであり、OKM によって生成されます。KMA には、FIPS 140-2 レベル 3 の認定を受けた HSM である Sun Crypto Accelerator 6000 PCIe カードを含めることができます。KMA にこの Hardware Security Module がある場合、鍵は HSM によって作成されます。それ以外の場合、暗号化操作では、Solaris 暗号化フレームワークのソフトウェアトークンプロバイダが利用されます。詳細については、242 ページの「鍵ポリシー」を参照してください。

鍵のライフサイクル

鍵ポリシーの計画で決定する事項に関しては、鍵のライフサイクルが主な構成項目です。鍵のライフサイクルの運用フェーズの期間は、データ保持の必要性および TDE マスター鍵が再度鍵に作成される頻度に基づいて選択するようにしてください。詳細については、20 ページの「鍵のライフサイクル」を参照してください。

> **注 –** TDE の DDL は、OKM 内のスキーマ暗号化ダイアログと同様に、さまざまな鍵サイズのマスター鍵の仕様をサポートします。OKM で使用できるのは、AES 256 ビット鍵のみです。

鍵ポリシー暗号化期間

鍵ポリシー暗号化期間は、ライフサイクルが保護および処理 (暗号化および復号化) 状態のときに鍵を使用する期間を定義します。この期間は、マスター鍵が再度鍵に作成されるまでの、マスター鍵を使用する期間に対応するようにしてください (たとえば、PCI の場合、最大 1 年間)。

鍵ポリシー暗号化有効期間

鍵ポリシー暗号化有効期間は、鍵のライフサイクルが処理のみ (復号化のみ) 状態のときに、マスター鍵を使用したデータの復号化のために割り当てられている残りの時間です。この期間の長さは、TDE マスター鍵によって保護されるデータのデータ保持要件と一致するようにしてください。通常、この値は、企業のデータ保持ポリシーに対応する年数となります (たとえば、米国の税務記録の場合、保持期間は 7 年間です)。

鍵の再作成操作はまれにしか行わないため、新しい鍵を生成する頻度は、TDE とは関係がないはずです。これが問題となる場合は、鍵ポリシーの暗号化期間を長くするか、鍵の再作成の頻度を低くすることを検討します。また、OKM の鍵プールサイズ設定パラメータを増加させて、利用可能な鍵のより大きいプールを維持管理するように KMA に指示することもできます。

必要に応じて、さまざまなタイプのデータベースで使用するために、複数の鍵ポリシーを定義できます。

鍵グループを使用した鍵アクセス制御

複数のデータベースインスタンスまたは複数のエージェントがさまざまな目的で OKM のクラスタにアクセスする場合、OKM によって管理される鍵へのアクセスを制御する必要がある場合があります。

すべての OKM エージェントには、少なくとも 1 つの鍵グループが割り当てられており (デフォルトの鍵グループへの割り当ては必須です)、このグループにより、グループ内の鍵へのアクセスが認証されます。エージェントのデフォルトの鍵グループは、pkcs11_kms プロバイダのエージェントがその中で鍵を作成する唯一の鍵グループです。

マスター鍵をデータベースインスタンスまたはホスト間で共有する必要がない場合は、複数の鍵グループの使用を検討してください。例としては、ある鍵グループを本稼働データベースインスタンスで使用し、別の鍵グループを開発 / テストのデータベースで使用して、分離が保証されるようにします。テストデータベースの鍵グループのエージェントは、本稼動データベースのマスター鍵を使用しようとすると、OKM によってブロックされます。また、そのような試行は OKM の監査ログにフラグが付けられ、本稼動データベースに支障を与える可能性がある構成エラーが存在することを示す場合があります。

TDE は、鍵ラベルの命名規則を使用したマスター鍵の分離も提供します。PKCS#11 の仕様では、鍵のラベルは一意である必要はありません。ただし、OKM は、ラベルが一意になるように強制し、OKM のクラスタでラベルの名前空間の有効範囲がグローバルになるようにします。別個のデータベースインスタンスの別個のマスター鍵の間でラベルの衝突が発生した場合は、最初に作成されたラベルが常に返されます。これが望ましい動作ではない場合は、エージェントを分離するための手段として鍵グループを使用することを検討してください。

同一のラベルを共有する、別の鍵グループに属する鍵にエージェントがアクセスしようとすると、OKM によって拒否されます。これは、鍵の再作成操作の際に捕捉されますが、回避方法は衝突しない別のラベルが生成されるまで鍵を再作成することです。

鍵およびデータ破棄に関する考慮事項

データ保持要件に一致させるためのデータの破棄は、TDE のマスター鍵の破棄から開始できます。これらの鍵を破棄する方法とタイミングは、重要な計画項目です。OKM では、これを行うことができ、これらの鍵が含まれている OKM のバックアップを追跡することもできます。OKM のバックアップの管理は、障害回復計画および鍵の破棄計画の両方の項目です。

TDE 用の OKM クラスタの構成

次のリストは、TDE 用に OKM クラスタを構成するために必要なタスクを要約しています。

注 –

- これらのタスクでは、適切な管理ユーザーおよび役割によって構成された動作している OKM クラスタがあることを想定しています。
- OKM クラスタ内のすべての KMA では、少なくとも OKM 2.4.1 および Replication Version 13 が実行されている必要があります。

1. 鍵ポリシーを定義します。

   次を参照してください。

   - 242 ページの「鍵ポリシー」
   - 415 ページの「鍵ポリシーに関する考慮事項」。
2. グループ定義を定義します。

   鍵グループに鍵ポリシーを割り当て、グループにわかりやすい名前を付けます。

   次を参照してください。

   - 250 ページの「鍵グループ」
   - 416 ページの「鍵グループを使用した鍵アクセス制御」
3. エージェントを構成します。

   次を参照してください。

   - 411 ページの「OKM の PKCS#11 プロバイダ」。
   - 295 ページの「「Agent List」メニュー」
4. 各エージェントをデフォルトの鍵グループと関連付けます。

   266 ページの「「Key Group Assignment to Agents」メニュー」を参照してください。

エージェント ID

エージェント ID は、その構成において意味を持つものにできますが、そのエージェントに関連付けられるデータベースインスタンスの Oracle ユーザーに対応するようにしてください。

パスフレーズ

このパスフレーズは、ウォレット (たとえば、pkcs11_kms トークン) を開く DDL 文を使用して OKM で認証するために、Oracle のホストにも設定されるため、強いパスフレーズを選択します。パスフレーズの要件については、299 ページの「エージェントの作成」を参照してください。

共通のエージェント ID を共有する複数の Oracle RAC ノードからの場合に加えて、TDE の「ウォレット」を開く必要がある場合に、常にパスワードベースの認証を利用できるようにするために、OneTimePassphrase フラグを「false」に設定するようにしてください。セキュリティーを最大にする場合は、デフォルト値の「true」に設定できますが、単一ノードの Oracle Database 構成でのみ動作し、Oracle RAC では動作しません。OneTimePassphrase が true の場合、エージェントが認証に最初に成功したときにのみ、エージェントの X.509 証明書が返されます。pkcs11_kms プロバイダは、パスフレーズで保護された PKCS#12 ファイルに X.509 証明書の非公開鍵を安全に格納します。その後、X.509 証明書および対応する非公開鍵は、エージェントの OKM とのトランザクションに使用されます。pkcs11_kms プロバイダが格納するその他の情報については、kmscfg (1M) を参照してください。

鍵グループ

TDE 用に定義された鍵グループにエージェントを割り当てます。pkcs11_kms プロバイダは、鍵の作成操作 (鍵の再作成操作を含む) に対してデフォルトの鍵グループのみをサポートします。エージェントに関連付けられているデフォルト以外の追加の鍵グループは、それらのグループの鍵からの鍵取得のみが許可されます。この機能は、読み取り専用 / 復号化専用のデータベースシナリオで活用できます (マスター鍵を生成することはないが、マスター鍵にアクセスする機能のみが必要なセカンダリデータベースをサポートする場合など)。

pkcs11_kms のインストールおよび構成

OKM の PKCS#11 プロバイダである pkcs11_kms を Oracle データベースサーバーにインストールおよび構成する必要があります。インストールの手順については、pkcs11_kms のディストリビューションに同梱されているドキュメントを参照してください。pkcs11_kms のディストリビューションは、次の URL から入手できます。

http://www.myoraclesupport.com

TDE のための構成

TDE のマスター鍵を必要とする Oracle Database ノードに pkcs11_kms プロバイダを構成する必要があります。次の手順を行って、pkcs11_kms プロバイダを構成します。

1. O/S ユーザーに関する考慮事項

   Oracle Database のユーザーアカウントを使用して、エージェントと pkcs11_kms プロバイダを構成します。これは、O/S ユーザーの特殊な権限を必要としません。ホストで「複数の Oracle ホーム」がサポートされる場合は、各 Oracle Database ソフトウェア所有者のユーザーアカウントに応じて pkcs11_kms トークンを構成する必要があります。詳細は、『Oracle Database インストレーションガイド 11g Release 2』を参照してください。

2. kmscfg ユーティリティーは、1 ユーザーごとに 1 つのスロットの構成を一度に作成します。個別のユーザーに対して追加のスロット構成を定義することはできますが、1 プロセスでアクティブにできるのは 1 つのみです。各スロット構成は、そのユーザーに定義されているほかのスロットから、およびほかのユーザーから鍵ラベル名を分離します。スロット構成は、KMSTOKEN_DIR 環境変数を使用して制御し、代替のスロット構成およびファイルシステムの場所を定義できます。KMSTOKEN_DIR 環境変数は、シェルで永続的になるようにシェル設定ファイル (.bashrc など) 内に設定して、データベースが PKCS#11 操作を実行する前に常に設定されているようにしてください。エージェントプロファイルを Oracle RAC ノード間で共有する必要がある Oracle RAC の場合は、KMSTOKEN_DIR 環境変数を使用し、適切な共有ファイルシステムパスを使用してプロファイルを作成するように kmscfg に指示します。

   スロットの構成および実行時の情報のために、ファイルシステムのストレージスペースを割り当てます。Oracle RAC の使用を計画している場合は、Oracle RAC ノードの各ユーザーが読み取り可能および書き込み可能なアクセス権を持つ共有ファイルシステムの場所に、プロファイルを定義する必要があります。各エージェントログが拡張可能になるように領域要件を割り当てます。このログファイルは自動的に作成され、トラブルシューティングのツールとして役に立ちます。KMSAgentLog.log ファイルによって消費される領域は、logadm (1M) などのツールを使用して管理できます。ほとんどの構成では、各エージェントのプロファイルディレクトリに 10M バイトを割り当てれば十分です。

3. kmscfg (1M) ツールを使用して、pkcs11_kms プロバイダを初期化します。このステップでは、あとで pkcs11_kms トークンに関連付ける OKM エージェントにプロファイルを定義します。

```
# kmscfg

Profile Name: oracle

Agent ID: oracle
```

```
KMA IP Address: kma1
```

この時点で、PKCS11 スロットが定義され、OKM での認証を検証できます。

4. TDE が自動オープンウォレットを使用するように構成する場合は、この付録の最初に参照したドキュメント『Oracle Advanced Security Transparent Data Encryption Best Practices』で説明されている手順に従ってください。

Oracle Database の TDE の構成

各 Oracle データベースサーバーは、サポートされる pkcs11_kms プラットフォームで 11.2.0.2 を実行している必要があります。必須のパッチ 12626642 をインストールする必要があります。このパッチは、次の URL から入手できます。

https://updates.oracle.com/download/12626642.html

インストールが完了したら、TDE アクセスのために共有ライブラリファイルを構成する必要があります。

`/opt/oracle/extapi/32|64/hsm/<vendor>/<version>/libname.ext`

ここで、<vendor> は「Oracle」、<version> は PKCS#11 ライブラリの「1.0.0」バージョンです。ライブラリ自体のファイル名は、/usr/lib/pkcs11_kms.so へのシンボリックリンクです。

継続的な運用

次のセクションでは、繰り返し行う OKM および TDE の運用タスクについて説明します。

汎用マスター鍵の生成および鍵の再作成

Oracle Wallet からのマスター鍵のマイグレーション

以前のウォレットは保持する必要があり、OKM によって新しいマスター鍵が生成されて、鍵管理システムによって安全に保護されます。

この付録の最初に参照したドキュメント『Oracle Advanced Security Transparent Data Encryption Best Practices』を参照してください。

TDE は、各マスター鍵を識別する一意の鍵ラベルを生成します。実際の鍵の値は、pkcs11_kms トークンから TDE に渡されるまで、標準テキストとして公開されません。「作成された」鍵は、アクティブ状態の (安全に複数の KMA にレプリケートされた) AES 256 ビット鍵のプールから取得されます。その後、この鍵は、PKCS#11 トークンによって使用される特定のエージェントに応じて、OKM 鍵ポリシーと関連付けられます。OKM は、ポリシーによって規定された鍵のライフサイクルに応じて鍵を管理します。

鍵の再作成操作

Oracle Database 管理者は、鍵のライフサイクルによって要求される前に、鍵の再作成操作を実行する必要があります。そうしない場合、データベースは起動しません。

この操作を実行するために使用される DDL については、Oracle Database および TDE の各種ドキュメントを参照してください。鍵の再作成は、Oracle Enterprise Manager を使用して実行することもできます。

OKM ポリシーベースの鍵の期限切れによる鍵の再作成

鍵が運用後状態に達した場合、TDE によって各鍵取得が行われると、運用後鍵を取得したことを示す警告が OKM 監査ログに出力されます。これらの監査メッセージが存在する場合は、そのデータベースインスタンスのマスター暗号化鍵を鍵を再作成する時期であることを示しています。OKM の監査メッセージは、Oracle Database インスタンスおよび運用後状態に達したマスター暗号化鍵の識別を容易にするために、特定のエージェントと取得されている鍵を識別します。この処理の自動化をサポートするために、SNMP v3 の inform または SNMP v2 の trap を使用した通知を OKM に構成できます。

pkcs11_kms プロバイダは、鍵が運用後状態に達したことを PKCS#11 コンシューマに通知しようとします。これは、マスター鍵に対して PKCS#11 の「CKA_ENCRYPT」属性を false に設定することにより行われます。

現在、Oracle Database 11gR2 は、暗号化期間が期限切れになったあとも、鍵を使用したデータの暗号化を継続します。次のエラーが警告ログに出力されたときにこの動作を確認できます。

```
HSM heartbeat died. Likely the connection has been lost. PKCS11
function C_EncryptInit returned

PKCS11 error code: 104
```

```
HSM connection lost, closing wallet
```

このエラーが発生したら、次のアクションのいずれかを行います。

- Oracle Database エージェントに関連付けられている OKM 鍵ポリシーに、非常に長い暗号化期間を使用します。
- pkcs11_kms プロバイダの動作を変更して、鍵の状態の確認を無効にします。

  pkcs11_kms トークンに関連付けられているユーザーに、次の環境変数を設定します (通常は、oracle ユーザーのプロファイル)。

  ```
  #export PKCS11_KMS_ALLOW_ENCRYPT_WITH_DEACTIVATED_KEYS=1
  ```

  この変数を設定すると、HSM を開くことができます。

  これにもかかわらず、TDE はその鍵の使用を継続し、自動的な鍵の再作成操作を行いません。運用後鍵の取得に関する監査警告を確認した OKM 管理者は、データベースインスタンスのマスター鍵を再作成する時期であることを DBA に通知する必要があります。

別の HSM ソリューションからの変換

別のベンダーの HSM ソリューションから OKM に変換するために必要な具体的な手順については、Oracle テクニカルサポートにお問い合わせください。

鍵の破棄

運用後フェーズに達した鍵を破棄する前に、OKM 管理者はその鍵が使用されなくなったことを検証する必要があります。

OKM 管理者は、運用後フェーズに入った鍵を定期的に破棄する責任があります。pkcs11_kms プロバイダを使用した鍵の削除は、OKM でサポートされておらず、オペレータの役割を割り当てられている OKM ユーザーに予約されている制限された操作です。鍵が破棄されたあとに、それを取得しようとすると失敗します (PKCS#11 の C_FindObjects 要求も含みます)。

Oracle RMAN または Oracle Data Pump、あるいはその両方をサポートするための鍵転送

Oracle RMAN または Oracle Data Pump、あるいはその両方を使用する場合、マスター鍵を別の OKM クラスタに提供する機能が必要となることがあります (たとえば、障害回復サイトにおいて、またはパートナーに対して)。OKM の鍵転送操作は、セキュリティー保護された鍵エクスポートサービスおよび鍵インポートサービスを使用して、これを容易にサポートします。詳細については、169 ページの「鍵転送」 を参照してください。

次の手順を実行します。

1. 転送元および転送先の OKM クラスタ間で鍵転送パートナーを確立します。
2. Oracle RMAN バックアップ、または Oracle Data Pump を使用してエクスポートされる暗号化データをサポートするためにエクスポートする TDE マスター鍵を識別します。
3. 転送元 OKM クラスタから鍵をエクスポートします。これにより、セキュリティー保護された鍵エクスポートファイルが作成されます。
4. エクスポートされた鍵ファイルを転送パートナーに転送します。
5. 転送先の転送パートナーは、鍵を自身の OKM クラスタにインポートします。

Oracle RMAN の復元または Oracle Data Pump のインポートを実行して、鍵を必要とするデータベースインスタンスを再作成します。これには、インポートする場所で TDE を OKM で使用するために必要な構成ステップが必要です。その後、復元またはインポートの操作は OKM にアクセスして、データベースインスタンスによって使用される列またはテーブル領域の鍵を復号化するために必要な汎用マスター鍵を取得します。

管理

システムがアクティブになったら、次のガイドラインを使用して、このソリューションを効果的に管理および監視します。

確認、監査、および監視

推奨事項は次のとおりです。

- TDE エージェントの OKM 動作履歴を確認および監視して、問題の検出に役立てます。
- 監査者は、OKM 監査イベントを使用して、TDE が OKM クラスタからマスター鍵にアクセスしていることを確認できます。
- OKM 用に SNMP マネージャーを構成します。
- OKM の CLI を使用して、企業に固有のレポートを生成することを検討します。
- My Oracle Support および Oracle の拡張サービスに ASR 機能を統合することを検討します。

OKM 内の TDE マスター鍵の検出

GUI 管理ツールまたは CLI を使用して、OKM 内の TDE マスター鍵を検出できます。TDE はマスター鍵のラベルを生成し、OKM はデータユニットの External Tag 属性を使用してこの値を格納します。TDE のマスター鍵生成 (鍵の再作成操作を含む) では、OKM クラスタ内に新しいデータユニットオブジェクトおよび鍵オブジェクトが常に作成されます。

TDE マスター鍵を検出するには、次を行います。

1. OKM データユニットに対してクエリーを実行し、ExternalTag フィルタを使用してリストをフィルタします :「ExternalTag」が「ORACLE.TDE」で始まる。すべての TDE 鍵ラベルはこの文字列で始まるため、これにより、TDE によって作成された OKM データユニットのリストが生成されます。各 OKM データユニットには、単一の TDE マスター鍵が関連付けられます。これらの鍵は、GUI を使用して表示し、ライフサイクルの状態およびその他のプロパティー (鍵グループ、エクスポート / インポートのステータス、破棄された鍵が含まれている OKM バックアップなど) を確認できます。OKM の CLI を使用する場合、次のようになります。

   ```
   >okm listdu --kma=acme1 --user=joe \
      --filter="ExternalTag=ORACLE.TDE"
   ```

2. 複数の Oracle Database インスタンスが 1 つの OKM クラスタを共有している場合、特定のデータベースに対応する鍵を識別するには、そのデータベースインスタンスに対応するエージェントの監査イベントに対してクエリーを使用することにより判別できます。フィルタを使用して、エージェントの監査履歴をフィルタします :「Operation が CreateDataUnit に等しい」。これにより、TDE マスター鍵の作成に対応する監査イベントのリストが生成されます。この監査イベントの詳細には、マスター鍵の特定のデータユニットを識別するために必要な情報が示されます。OKM の CLI を使用する場合、次のようになります。

   ```
   >okm listauditevents --kma=acme1 --user=joe \

   --filter="Operation=CreateDataUnit"
   ```

障害追跡

マスター鍵を取得できない場合、Oracle Database は次のいずれかのエラーを報告します。

- ORA-28362
- ORA-06512

これらのエラーが発生した場合は、次の診断手順を行って問題を特定します。

1. $ORACLE_BASE/diag/rdbms/$SID/$SID/trace/alert_$SID.log ファイルを確認します。このファイルには、暗号化ウォレットにアクセスするために使用された「alter」DDL 文に関連する成功 / 失敗のメッセージが記録されます。
2. pkcs11_kms トークンの KMSAgentLog.log ファイルを確認します。
3. OKM の全般的なステータスを検査します。次をチェックします。
   - KMA はアクティブか ?
   - KMA はロックされているか ?
   - 鍵プールは枯渇しているか ?
   - KMA の ILOM/ELOM の障害
   - KMA コンソールのメッセージ
4. pkcs11_kms トークンのステータスが以前の状態と同じであるかどうかを検査します。
5. エージェントの OKM 監査イベントを調査することでエージェントのステータスを検査し、そのエージェントが登録され、有効になっていることを確認します。
6. Oracle Database のホストから OKM ノードへのネットワーク接続を検査します。
7. Oracle テクニカルサポートに問い合わせます。1 つまたは複数の KMA システムダンプの提供を要請されることがあります。

PKCS#11 操作を実行しようとしたときに、クライアントで「No Slots Available」エラーが発生する

1. kmscfg が実行されていることを確認します。
2. Solaris で、pkcs11_kms がインストールおよび構成されていることを cryptoadm を使用して確認します。

鍵を取得しようとしたときに、クライアントで CKA_GENERAL_ERROR エラーが発生する

1. エージェントにデフォルトの鍵グループがあることを検査します。
2. 詳細は、$KMSTOKEN_DIR/KMSAgentLog.log を確認します。

KMSAgentLog.log に「Could Not Open PKCS#12 file」エラーが出力される

エージェントのパスワードが OKM で変更されている可能性があります。$KMSTOKEN_DIR の <profile-name> ディレクトリを削除します。

pkcs11_kms 設定ディレクトリの消失

次の手順を使用して、消失または破壊された pkcs11_kms トークンプロファイルを復元します。

1. 419 ページの「TDE のための構成」で説明されている構成手順を行います。
2. **Solaris のみ** - OKM で次のデータユニットのフィルタを使用して、トークンのメタデータを取り込み直します :「ExternalTag」が「ORACLE.TDE」で始まる。
3. **Solaris のみ** - このリストの結果をファイル (たとえば、「du.lst」) に保存してから、次のシェルスクリプトを実行します。

```
for label in `awk '{print $2}' < du.lst `
do
    pktool list token=KMS objtype=key label="${label}"
done
```

用語集

A

Advanced Encryption Standard (AES)
FIPS で承認された NIST 暗号化規格で、電子データの保護に使用されます。

AES
「Advanced Encryption Standard」を参照してください。

B

BOT
テープ開始位置 .

C

CA
「認証局 (CA)」を参照してください。

E

EKT
Enabling Key Token の略。有効化鍵トークン (デバイス鍵) のことです。KMS Version 1.x の用語。

F

FIPS
Federal Information Processions Standards (連邦情報処理標準) の略。National Institute of Standards and Technology (NIST、米国標準規格局) は、米国商務省の技術管理部内の非規制連邦機関であり、次のような標準規格や技術の開発および促進を行なっています。

- Computer Security Division and Resource Center (CSRC)

- Federal Information Processing Standards (FIPS、連邦情報処理標準)

詳細は、次の URL にアクセスしてください。
http://www.nist.gov/

G

GUI
グラフィカルユーザーインタフェース .

H

Hash Message Authentication Code (HMAC)
暗号化での HMAC (keyed-Hash Message Authentication Code) とは、暗号化ハッシュ関数と秘密鍵を組み合わせて計算される、メッセージ認証コード (Message Authentication Code、MAC) の一種です。

K

Key Management Appliance (KMA)
OKM ソフトウェアがロード済みの SunFire X2100-M2 サーバー。
Solaris 10 オペレーティングシステムが実装された、実証済みのデュアルコアプロセッサアプライアンスであり、ポリシーベースの鍵管理サービスおよび鍵プロビジョニングサービスを提供します。

KMA
「Key Management Appliance」を参照してください。

N

NIST
National Institute of Standards and Technology (米国標準規格局) の略。

O

OKM
「Oracle Key Manager」を参照してください。

OKM クラスタ
相互接続された 1 つ以上の KMA の集合。OKM クラスタ内のすべての KMA は、同一の情報を持ちます。ただし、ある OKM が停止している場合、または新たに作成された情報の一部が OKM クラスタ内のすべての KMA にはまだ伝播されていない場合はこの限りではありません。OKM クラスタ内の任意の KMA で実行された動作は、最終的に OKM クラスタ内のすべての KMA に伝播されます。

OKT
Operational Key Token の略。運用中鍵トークン (媒体鍵) のことです。KMS Version 1.x の用語。

Operator
システムの日常業務の管理を担当するユーザーの役割。

Oracle Key Manager (OKM)
鍵管理を提供するシステム。Oracle システムには、暗号化エージェントの代わりに鍵管理を提供する OKM コンポーネントがあります。

P

PC 鍵
テープドライブの暗号化モードでの読み取りと書き込みを有効にします。

R

Rijndael アルゴリズム
米国標準規格局 (NIST) によって Advanced Encryption Standard (AES) 用に選択されたアルゴリズム。「ラインダール」と読むこのアルゴリズムは、Vincent Rijmen と Joan Daemen という 2 人のベルギー人暗号研究者によって考案されたものであり、暗号名にはこの 2 人の姓が反映されています。

RSA
暗号化での RSA とは、MIT の Ron Rivest、Adi Shamir、および Leonard Adleman によって考案された公開鍵暗号化アルゴリズムです。RSA という略称は、この 3 人の姓の頭文字です。

S

Secure Hash Algorithms (SHA)
Secure Hash Algorithms は、米国国家安全保障局 (NSA) によって策定され、NIST によって米国連邦情報処理標準として公開された暗号化ハッシュ関数です。

Shamir の秘密の共有法
暗号化アルゴリズムの一種。秘密情報が分割され、それぞれの分割部分には一意の内容のみが含まれるため、秘密情報の再構築にはこれらの分割部分の一部またはすべてが必要になります。秘密情報を再構築するためにすべての分割部分を組み合わせることは現実的ではありません。このため、定足数またはしきい値スキーマが使用されています。

T

T10000 テープドライブ
T10000 テープドライブは、データの大容量ストレージとして設計された、小型のモジュラー型高性能テープドライブです。最大 500 G バイトの非圧縮データに対応できます。

Transparent Data Encryption (TDE)
機密性のあるデータベース情報の暗号化および復号化のサービスを提供する Oracle データベース管理システムの機能。

Transport Layer Security (TLS)
暗号化プロトコルの一種。Web 参照、電子メール、インターネットファックス送信、インスタントメッセージ、その他のデータ転送などを目的として、インターネット上のセキュリティー保護された通信を提供します。

U

UID
暗号化エージェントやユーザーなどの OKM 構成要素の一意の識別子として機能する文字列。

Ultra Tape Drive Encryption Agent
Ultra 準拠の暗号化テープドライブでは、鍵管理に Ultra Tape Drive Encryption Agent ソフトウェアを活用します。このようなドライブでは、テープボリュームで使用される鍵データを OKM から取得します。このため、BOT からの書き込みごとに、ボリューム上のデータの暗号化に新しい鍵データが使用されます。その結果、データユニットの定義がテープボリュームに割り当てられ、データユニットの外部 ID はボリュームシリアル番号になります。

UTC
Coordinated Universal Time (協定世界時) の略。

あ

暗号化
データを暗号に変換することです。暗号化は、データの安全性を確保するもっとも有効な方法の一つです。暗号化されたファイルを読み取るには、復号化を可能にする特殊な鍵またはパスワードにアクセスできる必要があります。

暗号化アクセラレータ
暗号化アクセラレータは、データ暗号化および復号化の処理速度向上を目的として使用されるハードウェアデバイス (カード) です。これにより、需要が高い状況でのシステム性能が向上します。

暗号化使用可能
デバイスでの暗号化をオンに設定して暗号化を行う機能を持つテープドライブ。

暗号化動作中
ドライブで暗号化機能がオンになっている状態の暗号化対応テープドライブ。

暗号化有効期間
鍵を暗号化に使用できる期間。鍵が最初にドライブに割り当てられた時点から開始されます。この値は、NIST 800-57 の「Originator Usage Period」に対応しています。

暗号法
暗号化テキストと呼ばれる判読不能の形式に情報を変換 (暗号化) することによって情報を保護する技術。特別な鍵を所有しているユーザーのみが、メッセージを元の形式に解読 (復号化) できます。

い

インターネットプロトコル (IP)
インターネット環境でデータの発信元から受信先への経路指定に使用されるプロトコル。

インターネットプロトコル (IP) アドレス
デバイスを識別してネットワーク経由でアクセスできるようにする 4 バイトの値。IP アドレスの書式は、ピリオドで区切られた 4 つの数値で表される 32 ビットの数値アドレスです。それぞれの数値は 0 ～ 255 の値を取ります。たとえば、IP アドレスは 129.80.145.23 のようになります。
「TCP/IP アドレス」としても知られています。

え

エージェント
鍵データを作成および取得するために OKM と対話するさまざまなタイプの暗号化エージェントを作成できます。StorageTek T10000 モデル A と B、T9840D、および HP LTO Gen 4 と Gen 5 の各テープドライブは、暗号化機能に対して使用可能にすると、暗号エージェントのタイプになります。

エージェント API
「エージェントライブラリ API」を参照してください。

エージェントライブラリ
エージェントライブラリは、鍵データを OKM から取り出すために、エージェントによって使用されます。

エージェントライブラリ API
エージェントライブラリによって提供される API。エージェントはこの API を呼び出します。

か

鍵
ここでは、鍵は対称データ暗号化鍵のことです。エージェントは、1 つ以上のデータユニットに対応するデータの暗号化を行うために、新しい鍵データを要求できます。鍵は単一の鍵グループに属しているため、その鍵グループに関連付けられているエージェントのみが、対応する鍵にアクセスできます。鍵には、その鍵が属している鍵グループに関連付けられている鍵ポリシーで規定された、暗号化と復号化の暗号化有効期間があります。鍵のタイプ、つまり鍵の長さとアルゴリズムは、暗号化エージェントによって指定されます。

鍵グループ
鍵グループは、鍵を整理して鍵ポリシーと関連付けるために使用されます。また、鍵グループは、暗号化エージェントによる鍵データへのアクセスを強制するためにも使用されます。

鍵入力
Oracle Key Manager によって生成されるランダムなビット文字列。キーボードを使用して入力するか、または購入します。鍵には、次のタイプがあります。

- デバイス鍵は、テープドライブの暗号化機能を使用可能にします。
- 媒体鍵は、テープカートリッジ上の顧客データを暗号化および復号化します。
- PC 鍵は、テープドライブの暗号化機能を使用可能にします。
- 通信鍵は、トークンからドライブへの LAN を介した転送中に、暗号化 (認証) を行うための別の層を媒体鍵に追加します。

- 分割鍵はドライブごとに一意であり、保護を実現するためにラップ鍵と連携します。
- ラップ鍵は、LAN 上の媒体鍵とトークンを暗号化します。

書き込み鍵
データをテープに書き込む場合に使用される媒体鍵です。

鍵転送パートナー
鍵転送パートナーとは、OKM 間でエクスポートされる鍵の受信側のことです。

鍵転送ファイル
鍵と関連データユニット (定義されている場合) が含まれるファイル。鍵データを OKM クラスタ間で移動する場合に使用されます。転送にかかわる双方で、交換の相手側となる鍵転送パートナーが設定されている必要があります。鍵転送ファイルは、転送される情報の機密性と完全性を確実にするため、署名および暗号化されます。

鍵ポリシー
鍵ポリシーによって、鍵に適用される暗号化有効期間の設定値が提供されます。各鍵グループには鍵ポリシーがあり、鍵ポリシーは 0 個以上の鍵グループに適用できます。ポリシーで指定された暗号化と復号化の暗号化有効期間によって、鍵の使用法が制限され、鍵の無効化、破棄など、鍵のライフサイクルイベントが発生します。

また、鍵ポリシーによって制御される鍵を、どのような状況でほかの鍵転送パートナーにエクスポートできるか、またはその他の鍵転送パートナーからインポートできるかも、鍵ポリシーで制御されます。

監査
「監査ログ」を参照してください。

監査者
システム監査証跡 (監査リストイベントと KMA セキュリティーパラメータ) を表示できるユーザーの役割。

監査ログ
OKM クラスタでは、システム全体で発生する監査可能なすべてのイベントに関するログを維持します。エージェントは、監査可能なイベントについて、このログにエントリを追加できます。

く

クラスタ
クラスタは、耐障害性、可用性、および拡張性を向上させるために単一システムにまとめられた一連の Key Management Appliance です。

クリティカルセキュリティーパラメータ
セキュリティー関連情報 (たとえば、暗号化の公開鍵と秘密鍵、パスワードや PIN などの認証データ) のことです。この情報が公開されたり変更されると、暗号化モジュールのセキュリティーが損なわれる可能性があります。

こ

コンプライアンス責任者
組織内のデータの流れを管理するユーザーのロール。データコンテキスト (鍵グループ) と、データの保護方法および最終的な破棄方法を決定する規則 (鍵ポリシー) を定義および配備できます。

さ

サイト
サイトは、各 OKM および暗号化エージェントの属性であり、ネットワークの近接性 (局所性) を示します。ローカルサイトの KMA がどれも応答しない場合、暗号化エージェントはまず同じサイトの KMA との通信を試みてから、別のサイトの KMA との通信を試みます。

し

システムダンプ
ユーザーによって開始される操作。すべての関連データが単一ファイルにまとめられ、ユーザーがこの操作を開始したマシンにそのファイルがダウンロードされます。ダウンロードが完了すると、ファイルは KMA から削除されます。

証明書
証明書はデジタル署名されたドキュメントで、所有者の承認状況と名前の妥当性検査に使用されます。このドキュメントは、特殊な形式のデータブロックで構成されており、認証に必要な証明書の所有者名 (サブジェクト DN)、シリアル番号、有効期間、所有者の公開鍵、発行者の DN、および発行者のデジタル署名が含まれます。発行者は、所有者の名前がドキュメントの公開鍵に関連付けられている名前であることとを保証します。

自律ロック
自律ロック解除が使用可能の場合、ロックされている KMA のロックを解除するには、定足数のセキュリティー責任者が必要です。使用不可の場合は、任意のセキュリティー責任者が KMA のロックを解除できます。

せ

セキュリティー責任者
セキュリティー設定値、ユーザー、サイト、および転送パートナーを管理するユーザーの役割。

セキュリティーポリシー
組織データの機密性、データにアクセスする可能性のある各種実体、およびアクセスの管理と制限に適用される規則を厳密に記述したもの。

ゼロ化
データを回復できないようにデータストレージの内容を変更または削除することによって、電子的に格納されたデータ、暗号化鍵、およびクリティカルセキュリティーパラメータを消去すること。

た

タスクの異常終了 (不正終了)
コンピュータの処理タスクを停止する、ソフトウェアまたはハードウェアの問題。

つ

通信鍵
トークンからドライブへの LAN を介した転送中に暗号化および認証を行うための別の層を追加します。

て

データユニット
データユニットは OKM 内部の抽象的な構成要素で、OKM ポリシーや暗号鍵に関連付けられたストレージオブジェクトを表します。データユニットの具体的な定義は、データユニットを作成した暗号化エージェントによって定義されます。テープドライブの場合、データユニットはテープカートリッジです。

定足数メンバー
保留中の定足数操作を表示および承認するユーザーの役割。

デバイス鍵
テープドライブでの暗号化を有効にします。KMS Version 1.x の用語。

と

トークン
KMS Version 1.x の用語。
トークンとは、Ethernet 接続のトークンベイに接続される、コンパクトなインテリジェントデバイスです。トークンには、次の 2 つの役割があります。

- 有効化鍵トークン
- 運用中鍵トークン

トークンベイ
KMS Version 1.x の用語。
物理トークンを格納し、1 つまたは 2 つのトークンに対して背面のブラインドメイトコネクタ経由で電源と接続を提供するシャーシのことです。トークンベイは、標準 19 インチラック (1U フォームファクタ) と互換性があります。トークンベイには、デスクトップ型とラックマウント型の 2 つのタイプがあります。

に

認証局 (CA)
認証局は、エンドユーザーの登録および証明書の発行を行います。また、エンドユーザーの下に CA を作成することもできます。KMA 自体が認証局として機能し、ユーザー、エージェント、およびその他の KMA に対して証明書を発行します。

ね

ネットワーク
ソフトウェアおよびハードウェアによるリンクを介してデータ処理デバイスを相互に接続し、情報の交換を容易にするノードと分岐の配置。

は

媒体鍵
テープカートリッジ上の顧客データを暗号化および復号化します。

バックアップオペレータ
データと鍵のセキュリティー保護と格納の責任を負うユーザーの役割。

バックアップ鍵ファイル
バックアップ処理中に生成されるファイルで、バックアップファイルの暗号化に使用される鍵が格納されます。このファイルは、システムマスター鍵を使用して暗号化されます。マスター鍵は、定足数の鍵分割資格を使用して、コアセキュリティーバックアップファイルから抽出されます。

バックアップファイル
バックアップ処理中に作成されるファイルで、KMA の復元に必要なすべての情報が含まれています。バックアップ専用に生成された鍵を使用して暗号化されています。鍵は、対応するバックアップ鍵ファイルに格納されます。

ほ

ボリュームシリアル番号
テープボリュームの特定に使用される、6 文字の英数字ラベル。

ゆ

有効化鍵
テープドライブを使用可能にするために使用される、64 文字の一意の鍵。「PC 鍵」も参照してください。

よ

読み取り鍵
データをテープから読み取る場合に使用される媒体鍵です。

ら

ラップ鍵
LAN 上およびトークン上の媒体鍵を暗号化します。

索引

L

M

N

O

P

Q

R

S

T

U

あ

い

う

え

お

か

き

く

け

こ

さ

し

せ

そ

た

つ

て

と

に

ね

は

ふ

ほ

め

や

ゆ

よ

ら

る

ろ