LANDesk® System Manager 8.6

インストールおよび導入ガイド

本書の内容は、明示か黙示かを問わず、保証やライセンスを構成するものではありません。LANDesk は、特定の目的に対する整合性、商品性、知的財産権または第三者あるいは LANDesk のその他の権利への非侵害を含むがそれらに限定されず、のその他の権利への非侵害を含むがそれらに限定されず、それらの保証やライセンス、および他のすべての責任を負いません。LANDesk の製品は、医療、救命、または生命維持装置での使用を意図したものではありません。読者は、第三者が本書に関連する可能性がある知的財産権、およびここで説明された技術を所有することを認識し、LANDesk の責任とは無関係に、適切な弁護士の助言を求めることをお勧めします。

LANDeskは、本書および関連する製品の仕様および説明書をいつでも予告なしに変更する権利を保有します。LANDeskは、本書の使用に関する保証を行わず、本書に発生しうるいかなる間違いの責務を負わないことを前提とし、ここに記載されている情報を更新する責務を負いません。

目次

概要

本書では、コンピュータの管理を容易にし、一般的なコンピュータの問題をトラブルシューティングして、TCO を削減する製品である LANDesk® System Manager
をインストールし、導入するプロセスについて詳しく説明します。

この概要で説明する内容は次のとおりです。

このリリースの機能

コンピュータ業界の発展とともに、コンピュータ
システムはより複雑になり、管理が難しくなってきました。長年の間コンピュータの維持と修理にかける時間は、最初に購入した価格以上に総所有コスト（TCO）を増加させます。LANDesk® System Manager はコンピュータの管理を容易にし、一般的なコンピュータの問題をトラブルシューティングすることによって、TCO を削減する製品です。

- **システム インベントリの表示**：System Manager
  は、コンピュータのハードウェアとソフトウェアの構成について広範な情報を提供します。
- **コンピュータのヘルス ステータスの監視**：System Manager
  は、コンピュータが警告または危険な状態になったときに、温度、電圧、空きメモリ、空きディスク容量などの項目について報告します。
- **システム イベントのアラート受信**：System Manager
  は問題をユーザに通知するために各種のアラート方法を使用します。
- **パフォーマンスのリアルタイム監視または履歴の監視**：System Manager
  は、ドライブ、プロセッサ、メモリ、サービスなどの各種のシステム
  オブジェクトのパフォーマンスを監視します。指定したカウンタが上限または下限のしきい値、つまり、あらかじめ定義した回数を超えたときに通知を呼び出すようにアラート
  アクションを設定できます。
- **現在のプロセスとサービスの監視**：System Manager
  では、実行中のサービスとそのステータスを表示したり、サービス
  ステータスへの変更を通知するためにアラート アクションを設定できます。
- **リモートからのコンピュータの電源オン/オフ、および再起動**：System Manager
  は、その機能がサポートされているシステムでリモート電源管理を管理者コンソールから有効にできます。
- **スケジュールされたタスク表示**：一元化された場所から、すべてのエージェント導入、検索、

- **拡張された OS サポート**：
  多様な環境にあるすべてのデバイスを単一のコンソールから管理します。Windows 2000、2003、および XP Professional、Red Hat Linux、SUSE Linux、HP-UX、AIX をサポートします。詳細については、フェーズ 1「システム要件」を参照してください。
- **Intel* AMT と Intelligent Platform Management Interface (IPMI) のサポート**：System Manager は、アウトオブバンド (OOB) 通信によってあらゆるシステム状態のネットワーク デバイスをリモート管理する機能を提供するハードウェア ベースの管理コンポーネントをサポートします。デバイスが企業ネットワークに接続しており、スタンバイ電源が入っている限り、インベントリへのアクセス、リモート診断情報の表示、そのシステムのリモート再起動が行えます。
- **ブレード サーバ サポート**；ブレード サーバとブレード シャーシ管理モジュール (CMM) に対する管理機能とインベントリ機能の両方を含むサポート。
- **スクリプト作成ツール**： デバイスにカスタム タスクをスケジュールして実行できます。
- **タスク スケジューラ**：データの整合性と拡張性が強化された単一のデータベース スキーマにより、管理デバイスに関する詳細な情報にアクセスできます (Management Suite との完全な統合を含む)。この単一のスキーマの一部に含まれているのが、タスク スケジューラです。本バージョンより、すべてのタスク (検索、エージェント構成、) を共通のウィンドウで表示できるようになりました。このウィンドウから、スケジュールの再設定、スケジュールの変更、スケジュールの繰り返しの設定を行えます。
- **役割ベース管理**：
  ユーザの組織内の役割に基づいて、ユーザのツールおよびデバイスへのアクセスを設定します。役割ベースの管理によって、表示や管理できるデバイスの範囲および実行できるタスクを割り当てます。
- **非管理デバイス検索**：
  さまざまな方法を使用したネットワーク上のデバイスの検索。本製品は、Windows または Linux を実行しているサーバ、ブレード サーバおよびブレード シャーシ、IPMI 対応サーバ、Intel AMT 対応サーバ、およびその他のネットワーク デバイスを識別します。デバイス検索をスケジュールして、新しいデバイスを定期的に検索できます。また、ネットワークにある管理されていないデバイスのレポートも生成します。
- **改善されたセキュリティ**：証明書を使用したセキュリティ モデルを使用して、デバイスは認可されたコア サーバおよびコンソールのみと通信できます。
- **ソフトウェア配布**：ソフトウェア アプリケーションのインストール処理またはデバイスへのファイル配布処理を自動化します。
- **レポート**：プランニングおよび戦略的解析に使用できる、あらかじめ定義されたサービス レポートが提供されています。
- **スケジュールされたタスク サポート**：スケジューラ サービスの複数ログインを提供し、エージェントを持たないデバイスでタスクを実行する際にデバイスを認証できるようになりました。これは、複数の Windows ドメインにあるデバイスを管理する場合、特に便利です。

本製品の基本情報

System Manager は、Windows 2000 Pro SP4、Windows XP Pro SP1、Windows* 2000/2003 サーバ、Red Hat Enterprise Linux v3 サーバ、SUSE Linux 9 サーバ、HP-UX および AIX サーバなど異なるオペレーティング

システムを実行するデバイスを管理し、これらのネットワークのオペレーティング
システムのデバイスを管理する共通のインタフェースを提供します。LANDesk® Management Suite や LANDesk® Server Manager など、LANDesk の他の製品と共存させることもできます。

製品用語

- **コア サーバ**：管理ドメインの中心。製品の主要なファイルおよびサービスはすべてコア サーバに置かれます。管理ドメインにはコア サーバを 1 台だけ配置できます。コア サーバは新しいサーバでも用途を変更したサーバでもかまいません。
- **コンソール**：メインのインターフェイスであるブラウザベースのコンソール。
- コア データベース： この製品は、データを管理するためにコア サーバに MSDE データベースを作成します。
- **管理デバイス**：
  製品のエージェントをインストールしているネットワークのデバイス。「デバイス」には、デスクトップ、サーバ、ラップトップ、モバイル ノート、ブレード シャーシなどが含まれます。1 台のコア サーバで数千台のデバイスを管理できます。
- **公開**： すべてのユーザが閲覧可能なアイテム (グループ、配布パッケージ、タスクなど)。ユーザが公開のアイテムを変更しても、その変更内容は公開のままになります。[公開グループ] は管理者権限を持つユーザが作成します。
- **非公開またはユーザ**：
  現在ログインしているユーザが作成したアイテム。これらは他のユーザには表示されません。非公開またはユーザのアイテムは、[マイ配信方法]、[マイ パッケージ]、[マイ タスク] ツリーに表示されます。管理者権限を持つユーザは、[非公開グループ] および [ユーザ パッケージ] と [ユーザ タスク] を表示できます。
- **共通**：他のユーザが表示可能なアイテム。ある共通アイテムの (変更を行って) オーナーシップを引き受けた場合、そのアイテムは 2 つのアイテムに分かれます。共通アイテムはそのまま残り、ユーザ アイテムが [ユーザ] フォルダに保存されます。そのアイテムの [ユーザ] インスタンスは、他のユーザには表示されなくなります。ユーザは表示可能な任意のタスクを [共通] とマークして、他のユーザと共有できます。そのアイテムのプロパティで [共通] オプションをクリアすると、そのタスクはそのユーザの [ユーザ タスク グループ] にのみ表示されます。

本製品をネットワークに適合させるには

本製品は、既存のネットワークのインフラストラクチャを利用して、管理するデバイスとの接続を確立します。小規模のネットワークと大規模なエンタープライズ環境のいずれを管理する場合でも、既存のデバイスを管理する作業が大幅に簡略化されます。

Management Suite または Server Manager と System Manager の使用方法

System Manager を持っていて Management Suite または Server Manager と共に使用する場合には、コア サーバ使用開始ユーティリティを使って、System Manager を使う製品の有効なユーザ名とパスワードを提供する必要があります。System Manager / Management

Suite をインストールすると、3 つの操作コンソールが与えられます。Management Suite Windows 32 コンソールと Web コンソール、および System Manager Web コンソールです。Server Manager コンソールには、Management Suite の 2 つのコンソールにはない機能を持つ 3 つのナビゲーション項目 (アラート、監視、ログ) が含まれます。

Management Suite を導入すると、Management Suite のインストールにより管理デバイスから System Manager エージェントが削除され、System Manager を導入すると、管理デバイスから Management Suite エージェントが削除されます。Management Suite を System Manager と共に実行する場合、Management Suite の構成機能には監視オプションが含まれます。

Management Suite または Server Manager がインストール済みのコンピュータへの System Manager のインストール方法

Management Suite または Server Manager がインストールされているコア サーバに System Manager を追加する場合、元の Management Suite または Server Manager と同じインストールを使用してください。

1. autorun.exe を開きます。
2. [今すぐインストール] をクリックします。
3. 言語を選択して、[OK] をクリックします。
4. [ようこそ] 画面が表示されます。[**次へ**] をクリックします。
5. 必要なら [変更] を選択して、[次へ] をクリックします。
6. LANDesk® Server Manager をクリックし、[次へ] をクリックします。
7. ウィザードの画面上の指示に従ってください。

コア サーバ システムの要求

どのサーバをコア サーバとしてセットアップするかを検討する際は、フェーズ 1「システム要件」リストの要件を考慮し、サーバが要件を満たしている、または超えていることを確認してください。前提条件チェッカーが自動的に確認します。

専用のコア サーバを推奨
ドメインを管理するためにコア サーバを通過するトラフィックの負荷を考慮し、各コア サーバを本製品のホスティング専用に設定することをお勧めします。

同じサーバに他の製品をインストールする場合は、短期間および長期間にわたってリソースの問題が発生する可能性があります。

プライマリ ドメイン コントローラ、バックアップ ドメイン コントローラ、または Aciteve Directory コントローラにはコア サーバ コンポーネントをインストールしないでください。

インストールおよび導入方法

製品メディアの自動実行機能を使用してインストールする場合、インストール前にコアが要件に準拠しているかをインストール
プログラムが自動的に検証します。システム全体に関わるアプリケーションを異種ネットワークにインストールして導入するには、セットアップ
プログラムを実行する前に慎重な方法を選択し、重要な計画を立てる必要があります。本書では、本製品をセットアップする方法を紹介しています。本製品を導入するには、その前に管理ニーズを簡単に明確化する必要があります。

導入方法の考慮事項

導入とは、ドメインに追加するサーバに管理機能を適用するプロセスのことです。本書では、導入については、さまざまな「フェーズ」で説明しています。

段階的導入方法では、デバイスおよびクライアントに対する管理を有効にするためにより体系的なアプローチが用意されています。このアプローチは、2 つの簡単な原則に基づいています。

- まず、既存のネットワークに与える影響が最も小さい製品コンポーネントから、影響が最も大きいコンポーネントの順に導入します。
- 次に、必要なトラブルシューティングを複雑にする可能性のある、一度にすべてのサービスを導入する方法ではなく、綿密な計画に基づいて段階的に本製品を導入します。

本書では、本製品の導入に役立てるため連続的にまとめています。第 1 章、フェーズ 1
の「管理ドメインの設計」を直接参照してください。各フェーズを連続的に実行する必要があります。

インストールおよび導入の概要

本書では、インストールおよび導入タスクを次の各フェーズにまとめてあります。各フェーズは本書の各セクションと対応しています。各セクションでは、インストールの該当部分について詳しく説明します。「」の章は、本製品をすぐに使いはじめることができるように、サービスの構成、コンソールの実行、デバイスの検索、デバイスの [マイ デバイス]
リストへの移動、管理デバイスのアクションの構成を行う方法を説明しています。詳細は本書のそれぞれの章を参照していただくことを前提に、この章は簡潔に書かれています。「はじめに」の章で取り上げている手順の中には、本書の他の章でも繰り返し説明しているものもあります。

フェーズ 1 の要約

インストールのフェーズ 1 では、次のタスクを実行して、管理ドメインを設計します。

- ネットワーク情報の収集
- ネットワークがシステム要件を満たすかどうかの確認

詳細については、本書のこの後にあるフェーズ 1「管理ドメインの設計」を直接参照してください。

フェーズ 2 の要約

フェーズ 2 では、次のタスクを実行して本製品をインストールします。

- コア サーバのインストール

詳細については、本書のこの後にあるフェーズ 2「コア
サーバとコンソールのインストール」を参照してください。

フェーズ 3 の要約

インストールのフェーズ 3
では、ネットワーク上のデバイスを検索し、本製品のエージェントを導入します。コンソールからエージェントをプッシュするか、またはサーバ共有からプルすることができます。

詳細については、本書のこの後にあるフェーズ 3
「デバイスへのエージェントの導入」を参照してください。

はじめに

概要

LANDesk® System Manager をご購入いただきありがとうございます。LANDesk® System Manager は、スタンドアロン型のデバイス管理アプリケーションです。デバイスを迅速かつ効果的に管理できるので貴重な時間を最大限活用でき、時間と費用を節約します。System Manager では、デバイスの中央管理、アクション (パワー サイクル、脆弱性の評価、またはアラートの設定) ごとのデバイスのグループ化、リモートからのトラブルシューティング、ネットワーク安全性の維持、および最新パッチによるデバイスの更新を行うことができます。

このマニュアルは、System Manager をすぐに使い始めることができるように、サービスの構成、コンソールの実行、デバイスの検索、[マイ デバイス] リストへの移動、管理デバイスのアクションの構成を行う方法を説明しています。

System Manager! は Web アプリケーションなので、ブラウザを使ってアクセスでき、リモート ワークステーションからサーバの管理を行えます。一般的な Web アプリケーションと同様に機能しますが、より使いやすくするために Windows 型の詳細なコントロール機能も備わっています。たとえば、あるコントロールの上にマウス ポインタを置いてダブルクリックまたは右クリックできます (Windows アプリケーションと同じ)。たとえば、[マイ デバイス] リストでは、サーバ名をダブルクリックして特定のデバイス情報にアクセスしたり、右クリックして実行可能なアクションを確認したりできます。

ここでは、System Manager を起動し、ネットワーク上のデバイスの検索、[マイ デバイス] リストに移動するサーバの選択、エージェントの導入、各種タスクのためのターゲット デバイス設定の方法をステップごとに説明します。

インストレーション プログラムの実行

インストール時には、自動実行ページで LANDesk® System Manager を選択します。詳しいインストール手順の説明は、『LANDesk Management Suite インストールおよび導入ガイド』の「フェーズ 3」「フェーズ 2」に記載されています。

System Manager のインストールが完了したら、いつでも !ProductName! を使い始めることができます。次の各セクションでは、コア サーバ使用開始ユーティリティの実行、サービスの設定、コンピュータの検索、[マイ デバイス] リストへのデバイスの移動による管理対象デバイスの指定、デバイスのグループ化、ユーザの追加、エージェントの導入といった必要なタスクの完了方法について説明します。これらのタスクが終了したら、System Manager の強力な機能セットがデバイス管理にどのように役立つかを探索してみましょう。

コア サーバのライセンス認証

コア サーバのライセンス認証を行うまで、製品を実行することはできません。

コア サーバの使用開始 ユーティリティは、次のことを実行するために使用します。

- 使用開始時に新しい System Manager コア サーバのライセンスを認証する
- 既存の System Manager コア サーバを更新する、試用版ライセンスから通常のライセンスに切り替える、Management Suite または System Manager にアップグレードする

各コア サーバには、そのコア サーバに固有の認可証明書が必要です。

このユーティリティは初めて再起動する時に自動的に実行されます。

コア サーバがインターネットに接続されている状態で、次の操作を実行します。

1. [スタート]、[プログラム]、[コア サーバの使用開始] の順にクリックします。ユーザ名とパスワードが入力されます。
2. ライセンス購入時に割り当てられた固有のユーザ名とパスワードを入力します。
3. [使用開始] をクリックします。

コア サーバは、HTTP で Software ライセンス サーバと交信します。プロキシ サーバを使用している場合は、ユーティリティの [プロキシ] タブをクリックし、プロキシ情報を入力します。コア サーバがインターネットに接続している場合、ライセンス サーバとの交信は自動で行われ、ユーザの操作は必要ありません。コア が接続されていない場合、再起動時に [閉じる] をクリックして、認証ファイルを licensing@landesk.com に電子メールで送ります。

定期的に、コア サーバはノード カウントの検証情報を ¥Program Files¥LANDesk¥Authorization Files¥LANDesk.usage ファイル内に生成します。このファイルは、定期的に LANDesk Software ライセンス サーバに送信されます。このファイルは XML

形式で、電子署名が済んでおり、暗号化されています。このファイルに手動で変更を加えると、ファイルの内容と Software ライセンス サーバに対する次の利用状況レポートが無効になります。

- コア サーバの使用開始
  ユーティリティは、ダイアルアップによるインターネット接続を自動で起動しません。ダイアルアップ接続を手動で起動してライセンス認証ユーティリティを実行した場合は、ライセンス認証ユーティリティはダイアルアップ接続を使用して利用状況のレポートを送信することができます。
- 電子メールでもコア サーバのライセンスを認証できます。Program Files¥LANDesk¥Authorization ディレクトリにある .TXT 拡張子のファイルを licensing@landesk.com に送信します。LANDesk カスタマ サポートは、ファイルを添付した電子メールを返信します。このメールには、コア サーバにその添付ファイルをコピーしてライセンス認証を完了する方法が記述されています。

ユーザの追加

System Manager
ユーザとは、コンソールにログインし、ネットワークで特定のデバイスを対象に特定のタスクを実行することができるユーザです。ユーザは役割ベースの管理機能で管理します。役割ベース管理を使用すると、製品ユーザに、ユーザの権限およびスコープに基づく特別な管理役割を割り当てることができます。「権限」は、ユーザが表示して使用できる製品ツールと機能を決定します。「スコープ」は、ユーザが表示して管理できるデバイスの範囲を決定します。さまざまなユーザを作成し、その権限およびスコープを管理要件に合わせてカスタマイズできます。たとえば、ヘルプ
デスクの役割を果たすユーザを作成し、この役割に必要な権限をユーザに与えることが可能です。詳細については、『System Manager ユーザーズ
ガイド』の役割ベース管理について扱っている章を参照してください。

製品をインストールすると、2 つのユーザ アカウントが自動的に作成されます
(下記を参照)。さらにユーザを追加する場合は、手動でユーザ
アカウントを作成してください。ユーザは実際にコンソールに作成されるわけではありません。代わりに、ユーザがコア サーバの Windows NT ユーザ環境で LANDesk Management Suite
グループに追加されると、そのユーザは [ユーザ] グループ (左側のナビゲーション
ペインで、[ユーザーの管理] をクリック) に表示されます。[ユーザ] グループには、コア サーバの LANDesk Management Suite グループに現在いるすべてのユーザが表示されます。

[ユーザ] グループには 2 つの既定ユーザがいます。既定ユーザの 1
つは「既定管理者」です。既定管理者は、本製品のインストール時にサーバにログインした管理者ユーザです。

既定ユーザのもう 1 つは「既定のテンプレート ユーザ」です。このユーザにはユーザ プロパティ
(権限およびスコープ) のテンプレートが含まれており、Management Suite
グループに追加された新規ユーザを設定するときに使用します。つまり、Windows NT
環境で該当するグループにユーザを追加すると、ユーザは [既定のテンプレート ユーザ]
プロパティに現在定義されている権限とスコープを継承します。既定のテンプレート
ユーザにすべての権限と既定の [すべてのコンピュータ] スコープが選択されていると、LANDesk Management Suite グループに配属される新規ユーザは [ユーザ] グループに追加され、Management Suite ツールおよびデバイスすべてにアクセスする権限があります。

既定のテンプレート ユーザのプロパティ設定を変更するには、[既定のテンプレート ユーザ] を選択し [編集]
をクリックします。たとえば、一度に多数のユーザを追加するが、ツールまたはデバイスのすべてではアクセスを認めない場合は、最初に既定のテンプレート ユーザの設定を変更し、LANDesk Management Suite グループにユーザを追加します (以下の手順を参照)。既定のテンプレート
ユーザは削除できません。

Windows NT で LANDesk Management Suite グループにユーザを追加すると、ユーザは、[ユーザ]
ウィンドウで [ユーザ] グループに自動的に読み込まれ、現在の既定のテンプレート
ユーザと同じ権限とスコープを継承します。ユーザの名前、スコープ、および権限が表示されます。また、ユーザ固有のログイン ID で名前を付けられた新規ユーザ サブグループが、[ユーザ
デバイス]、[ユーザ クエリ]、[ユーザ レポート]、および [ユーザ スクリプト]
の各グループに作成されます (管理者のみが各ユーザ グループを表示できることに注意してください)。

逆に、LANDesk Management Suite グループからユーザを削除すると、ユーザは [ユーザ]
リストには表示されなくなります。ユーザのアカウントはまだコア サーバに存在し、いつでも LANDesk Management Suite グループに再追加できます。また、[ユーザ デバイス]、[ユーザ クエリ]、[ユーザ レポート]、および [ユーザ スクリプト] の各グループのユーザ
サブグループは保持されるので、データを失わずにユーザを復元したり、他のユーザにデータをコピーしたりできます。

F5 を押して System Manager コンソールの [ユーザ]
フレームの表示を更新します。ユーザまたはドメイン グループを LANDesk Management Suite
グループに追加する方法、または新しいユーザ アカウントを作成する方法については、『System Manager *ユーザーズ*
ガイド』の役割ベース管理について扱っている章にある「製品ユーザの追加」を参照してください。

ユーザまたはドメインを LANDesk Management Suite グループに追加するには

1. サーバの [**管理ツール**]、[**コンピュータの管理**]、[**ローカル ユーザーとグループ**]、[**グループ**] ユーティリティの順にクリックします。
2. [**LANDesk Management Suite**] グループを右クリックし、[**グループに追加**] をクリックします。
3. [**追加**] をクリックし、ユーザを入力するかリストから選択します (複数選択可)。
4. [**追加**] をクリックし、[**OK**] をクリックします。

注意 : [**ユーザ**] リストのユーザ アカウントを右クリックして LANDesk Management Suite
グループにユーザを追加するか、[**プロパティ**]、[**所属するグループ**]、[**追加**]
の順にクリックしてグループを選択し、ユーザを追加することもできます。

ユーザ アカウントがもうサーバに存在しない場合は、最初にサーバに作成する必要があります。

新しいユーザ アカウントを作成するには

1. サーバの [**管理ツール**]、[**コンピュータの管理**]、[**ローカル ユーザーとグループ**]、[**ユーザ**] ユーティリティの順にクリックします。
2. [**ユーザ**] を右クリックし、[**新規ユーザ**] をクリックします。
3. [新規ユーザ] ダイアログで、名前とパスワードを入力します。

4. パスワード設定を指定します。
5. [**作成**] をクリックします。[**新規ユーザ**]
   ダイアログは開いたままなので、追加のユーザを作成できます。
6. [**閉じる**] をクリックしてダイアログを終了します。

LANDesk Management Suite グループにユーザを追加すると、コンソールの [ユーザ] グループに表示されます。

サービスと資格情報の設定

ネットワーク上のデバイスの管理を始めるには、System Manager に必要なデバイス認証資格情報を提供する必要があります。コアにある Configure Services ユーティリティ (SVCCFG.EXE) を使って、必要なオペレーティング システム、Intel* AMT、IPMI BMC の認証資格情報を指定します。インベントリの既定、PXE 待機キュー設定、LANDesk データベース設定なども指定できます。

設定には Configure Services を次のように使用します。

- データベース名、ユーザー名、およびパスワード(インストール時に設定)。
- 管理対象デバイスに対するジョブのスケジュールに必要な資格情報(複数の管理者資格情報セットを入力できます。)
- IPMI BMC の設定に必要な資格情報(BMC の資格情報は 1 セットしか入力できません。)
- Intel AMT 対応デバイスの設定に必要な資格情報(Intel AMT の資格情報は 1 セットしか入力できません。)
- サーバ ソフトウェアのスキャン間隔、メンテナンス、インベントリ スキャン保存日数、およびログイン履歴の長さ
- 重複デバイス ID の処理
- スケジューラ構成 (スケジュールされているジョブとクエリ評価の間隔を含む)
- カスタム ジョブ構成 (リモート実行タイムアウトを含む)

1. コア サーバで、[スタート]、[プログラム]、[LANDesk]、[LANDesk Configure Services] の順にクリックします。
2. [スケジューラ] タブをクリックします。
3. [ログインの変更] ボタンをクリックします。
4. 管理対象デバイス上で使用する資格情報 (通常はドメイン管理者アカウント) を入力します。
5. [追加]
   をクリックします。管理対象デバイス上で同じ管理者ユーザ名アカウントが有効になっていない場合は、必要に応じて他の資格情報を追加します。
6. [適用] をクリックします。
7. 環境に IPMI 対応のサーバがある場合は、[BMC パスワード] タブをクリックします。[パスワード] テキスト ボックスにパスワードを入力し、[パスワードの確認入力] テキスト ボックスにパスワードを再入力して OK] をクリックします。すべての管理対象 IPMI サーバで同じ BMC ユーザ名とパスワードを共有する必要があります。
8. Intel AMT 対応のデバイスがある場合、[Intel AMT 構成] タブをクリックします。[ユーザ名] テキスト ボックスに現在設定されている Intel AMT ユーザ名を、[パスワード] テキスト ボックスに現在設定されているパスワードを入力します。[パスワードの確認入力] テキスト ボックスにパスワードをもう一度入力してから [OK] をクリックします。

9. 必要に応じて、ソフトウェア スキャン間隔などのその他の設定を行います。
10. [OK] をクリックして変更を保存します。

詳細については、各 Configure Services のタブで [**ヘルプ**] をクリックしてください。

コンソールの実行

System Manager
には、ネットワーク上のデバイスを表示、設定、管理、保護するためのツールがすべて用意されています。コンソール内のツールを使用すると、配布されたパッケージをアンインストールできます。

コンソールの上部ペインには、現在ログインしているサーバとログイン時に使用したユーザ名が表示されます。[マイ デバイス] リストはコンソールのメイン
ウィンドウで、ほとんどの機能はまずここから開始します。左ペインには、使用できるツールが表示されます。コンソールの右ペインには、管理タスクを遂行できるダイアログや画面が表示されます。

コンソールの利点として、すべての機能が 1 つのリモート ロケーション
(お使いのワークステーションなど)
から実行できるので、日常の保守や問題のトラブルシューティングのために、サーバ室に足を運んだり、管理対象の個々のデバイスがある場所まで行く必要がなくなります。

コンソールは次の 3 つの方法で起動できます。

- コア サーバで、[スタート]、[すべてのプログラム]、[LANDesk]、[System Manager] の順にクリックします。
- リモート ワークステーションのブラウザで、URLとして「http://coreserver/LDSM」と入力します。
- ダッシュボードで、[LDSM コンソール] をクリックします。

デバイスの検索

[**検索構成**]
タブでは、検索構成の新規作成、既存の構成の編集または削除、および検索構成のスケジュールを行うことができます。各検索構成は、わかりやすい名前、スキャン対象となる IP
範囲、検索タイプで構成されます。

構成を作成したら、[**検索のスケジュール**] ダイアログで検索の実行時期を設定します。

1. 左側のナビゲーション ペインで、[**デバイス検索**] をクリックします。
2. [**検索構成**] タブで、[**新規**] ボタンをクリックします。
3. 以下に説明するフィールドに必要な情報を入力します。各フィールドへの入力が完了したら、[**追加**] ボタンをクリックして [**OK**] をクリックします。

以下に、[**検索構成**] ダイアログ ボックスの各構成要素を説明します。

- **構成名**：
  この構成の名前を入力します。構成名にはわかりやすい名前を指定して、構成内容をすぐに認識できるようにしてください。構成は 255 文字以下とし、次の文字は使用しないでください。″、+、#、&、または %。これらの文字を 1 つでも使うと、構成名は表示されません。
- **標準ネットワーク スキャン** :指定した範囲の IP アドレスに ICMP パケットを送信してデバイスを検索します。これは最も詳細な検索ですが、最も時間がかかります。既定では、このオプションには NetBIOS が使用され、デバイスに関する情報が収集されます。

  ネットワーク スキャン オプションには、デバイス検索が TCP パケット応答を通して OS タイプを検索する **IP fingerprint** オプションが用意されています。IP FingerPrint オプションを使用すると、検索処理が多少遅くなります。

  ネットワーク スキャン オプションには、SNMP を使ってスキャンするように設定可能な [**SNMP を使用する**] オプションもあります。[**構成**] ボタンをクリックして、SNMP 構成の情報を入力します。
- **LANDesk CBA 検索** :標準の管理エージェント (以前の Management Suite の Common Base Agent (CBA)) をデバイスで検索します。標準の管理エージェントにより、コアサーバがネットワーク上のクライアントを検索して、通信することができます。このオプションは、製品のエージェントをインストールしているデバイスを検索します。ルータは標準の管理エージェントと PDS2 トラフィックをブロックします。複数のサブネット間で標準 CBA 検索を実行するには、複数のサブネット間で指定のブロードキャストを許可するようにルータを設定する必要があります。

  CBA 検索オプションでは、デバイス検索がデバイス上の LANDesk Ping Discovery Service (PDS2) を検索する **LANDesk PDS2 検索**オプションも使用できます。LANDeskLANDesk® System Manager、Server Manager、およびLANDesk Client Manager などのソフトウェア製品は、PDS2 エージェントを使用します。ネットワーク上のデバイスにこれらの製品がインストールされている場合は、このオプションを選択してください。CBA 検出は Linux コンピュータではサポートされていませんが、PDS2 を選択すれば、エージェントをインストール済みの Linux コンピュータは検出が可能になります。
- **IPMI** : IPMI 対応サーバを検索します。IPMI は、管理可能なハードウェアにアクセスするためのメッセージとシステムインターフェイスを定義するために、Intel、* H-P、* NEC、* および Dell * が開発、規格化した仕様です。IPMI には、監視と復旧機能が含まれており、デバイスの電源のオン/オフまたは OS の動作状態に関係なく、多くの機能にアクセスできます。BMC が構成済みでない場合、BMC は IPMI 検出のために本製品が使用する ASF ping に応答しないことに注意してください。つまり、通常のコンピュータとして検出されることになります。クライアントをプッシュするときに、ServerConfig がシステムをスキャンして IPMI を検出し、BMC を構成します。
- **サーバ シャーシ** : ブレード サーバ シャーシ管理モジュール (CMM) を検索します。サーバ シャーシのブレードは、標準のサーバとして検索されます。
- **Intel* AMT** : Intel Active Management Technology をサポートするデバイスを検索します。
- **開始 IP** :スキャンするアドレス範囲の開始 IP アドレスを入力します。

- **終了 IP** :スキャンするアドレス範囲の終了 IP アドレスを入力します。
- **サブネット マスク** :スキャンする IP アドレス範囲のサブネット マスクを入力します。
- **追加** :ダイアログの下部の作業キューに IP アドレスの範囲を追加します。
- **クリア** : IP アドレス範囲のフィールドをクリアします。
- **編集** : 作業キューで IP アドレスの範囲を選択し、[**編集**] をクリックします。IP アドレスの範囲が作業キューの上にあるテキスト ボックスに表示され、範囲を編集したり、作業キューに新しい範囲を追加したりすることができます。
- **削除**:作業キューに対して選択した IP アドレスの範囲を削除します。
- **すべて削除** :作業キューからすべての IP アドレス範囲を削除します。

これで検索タスクの構成が完了しました。次に、ネットワークに接続されているデバイスを検索する準備として、検索タスクの実行をスケジュールします。

検索タスクのスケジュールと実行

[デバイス検索] タブの [スケジュール] ボタンをクリックすると、[検索のスケジュール] ダイアログが表示されます。このダイアログでは、検索を実行する時刻をスケジュールできます。検索タスクは、すぐに実行する、後で実行する、定期的に繰り返し実行する、または、1 度だけ実行して何度も繰り返し実行することのないようにスケジュールできます。

検索タスクをスケジュールしたら、[検索タスク] タブを表示して、検索ステータスを確認してください。繰り返し実行される検索タスクをスケジュールすることにより、ネットワークに新たに接続されたデバイスが自動的に検索されます。

[検索のスケジュール] ダイアログには、次のオプションがあります。

- 未スケジュール : タスクのスケジュールは設定しませんが、後で使用するために [検索構成] リストの中に残しておきます。
- すぐに開始 : できるだけ速やかにタスクを実行します。タスクの開始までに 1 分かかる場合もあります。
- スケジュールされた時刻に開始 :指定した時間にタスクを開始します。このオプションをクリックする場合は、次の情報を入力してください。
    - 時刻 : タスクを開始する時刻
    - 日付 : タスクを開始する日付。ロケールの設定によって、日付順序は「日/月/年」または「月/日/年」になります。
    - 実行周期 : タスクを繰り返し実行する場合は、[日単位]、[週単位]、[月単位] のいずれかを選択します。[月単位] を選択し、すべての月には存在しない日付 (たとえば 31 日) を選択した場合、その日付が存在する月のみにタスクが実行されます。

検索タスクをスケジュールするには

1. 左側のナビゲーション ペインで、[検出されたデバイス] をクリックします。

2. [検索構成] タブで、目的の構成を選択して、[スケジュール] をクリックします。検索スケジュールを設定して [保存] をクリックします。
3. [検索タスク] タブで、検索の進行状態を監視します。[更新] をクリックして、ステータスを更新します。
4. 検索が完了したら、[非管理] をクリックして上の [検出されたデバイス] ペインにすべての検索結果を表示します (このペインは自動的には更新されません)。

検出されたデバイスの表示

検出されたデバイスは、[検出されたデバイス] ペインでデバイスの種類別に分類されます。既定では [コンピュータ] フォルダが表示されます。別のカテゴリのデバイスを表示するには、左ペインでカテゴリのフォルダをクリックします。[非管理] をクリックすると、検出されたすべてのデバイスが表示されます。

- ブレード サーバ シャーシは [シャーシ] フォルダに表示されます。
- 標準のエンタープライズ デバイスは [コンピュータ] フォルダに表示されます。
- ルータとその他のデバイスは [インフラストラクチャ] フォルダに表示されます。
- Intel AMT 対応のデバイスは [Intel AMT] フォルダに表示されます。
- IPMI 対応のサーバは [IPMI] フォルダに表示されます。
- カテゴリのないデバイスは [その他] フォルダに表示されます。
- プリンタは [プリンタ] フォルダに表示されます。

注意： 一部の Linux サーバはオペレーティング システム名が一般の「Unix」と表示されます (または「その他」の場合もあります)。標準の管理エージェントを導入すると、これらのサーバは [マイ デバイス] リストの OS 名のエントリを更新し、完全なインベントリを表示します。
検出されたサーバを表示するには

1. [デバイス検出] ページの左ペインで、[コンピュータ] または表示する別の種類のデバイスをクリックします。検索結果が右ペインに表示されます。
2. 検索結果をフィルタするには、フィルタ アイコン をクリックし、検索する対象の一部を入力してから [検索] をクリックします。

名前の割り当て

ネットワーク スキャンによる検索を実行すると、返されるサーバにノード名 (またはホスト名) が割り当てられていない場合があります。これは、Linux を実行しているサーバによく見られます。[管理] を使用してサーバを [マイ デバイス] リストに移動するには、そのデバイスに名前を割り当てる必要があります。

1. [デバイス検索] ページで、名前の付いていないデバイスをクリックします。ノード名の列の空白部分をクリックする必要があります。
2. ツール バーの [名前の指定] をクリックします。
3. 名前を入力して [OK] をクリックします。

製品エージェントをデバイスにインストールすると、ホスト名が自動的にスキャンされ、コア データベースが正しい情報に更新されます。

[マイ デバイス] リストへのデバイスの移動

デバイスが検出されたら、手動で管理対象のデバイスを選択して、[マイ デバイス]
リストに移動する必要があります。デバイスを移動しても、そのデバイスにソフトウェアがインストールされるわけではありません。デバイスに対するクエリの実行、デバイスのグループ化、および [マイ デバイス]
リストでのデバイスの並べ替えが可能になるだけです。特定のデバイスを特定のアクションの「ターゲット」として指定します。これは多数の Web アプリケーションにある「買い物かご」モデルに類似しています。

1. [検出されたデバイス] ビューで、[マイ デバイス]
   リストに移動するデバイスをクリックします。複数のサーバを選択するには、Shift
   キーを押しながらクリック、または Ctrl キーを押しながらクリックします。
2. [ターゲット] ボタンをクリックします。[ターゲット] ボタンが表示されていない場合は、ツール
   バーの [<<] をクリックします。このボタンはツール
   バーの一番右端にあります。または、選択したサーバを右クリックし、[ターゲット]
   をクリックします。
3. 下のペインで、[管理] タブをクリックします。
4. 選択して、選択したデバイスを管理データベースに移動します。あるいは選択して、ターゲット
   デバイスを移動します。
5. [移動] をクリックします。

[移動] をクリックすると、デバイスが [マイ デバイス]
リストに移動され、デバイスの情報がデータベースに追加されます。情報がデータベースに追加されると、デバイス名、IP アドレス、OS
などに基づいてその情報に対するクエリおよびレポートの実行が制限付きで可能になります。

アクションのためのデバイスのグループ化

地域別、機能別などでデバイスをグループ化すると、それらのデバイスに対するアクションを迅速に実行できます。たとえば、特定の場所にあるすべてのデバイスのプロセッサ速度を確認することも可能です。

1. [マイ デバイス] リストで、[非公開グループ] または [公開グループ] をクリックしてから
   [グループの追加] をクリックします。
2. [グループ名] ボックスにグループの名前を入力します。
3. 作成するグループのタイプを選択します。
   - 静的 :
     グループに追加されたサーバ。これらのサーバは、削除されるか、ユーザがこれらのサーバを管理から除外するまでグループ内に属します。
   - 動的 : クエリで定義した 1 つまたは複数の条件に適合するサーバ。たとえば、1
     つのグループに現在警告状態にあるすべてのサーバを含めることもできます。これらのサーバは、グループに対して定義された条件を満たす限り、グループ内に属します。グループ クエリ条件を満たしたデバイスは、自動的にダイナミック グループに追加されます。
4. 終了したら、[OK] をクリックします。
5. デバイスを静的グループに追加するには、[マイ デバイス]
   リストの右ペインでデバイスをクリックし、[移動/コピー]
   をクリックします。次にグループを選択し、[OK] をクリックします。

管理対象デバイスの設定

デバイスを検索するだけでは、管理傘下に入れることにはなりません。コンソールからデバイスを完全に管理してヘルス状態のアラートを受け取るには、あらかじめサーバに管理エージェントをインストールしておく必要があります。既定のエージェント構成 (すべての管理エージェントをインストールします) をインストールするか、独自のエージェント構成をカスタマイズしてデバイスにインストールできます。(ヘルス アラートを受信するためにはエージェント構成に監視エージェントが含まれている必要があります。)

管理エージェントは、次のいずれかの方法でインストールできます。

- [マイ デバイス]
  リストでデバイスをターゲット指定し、そのデバイスにリモートでエージェントをインストールするようにエージェント構成タスクをスケジュールします。(以下の手順を参照)
- コア サーバの LDlogon 共有フォルダ (//coreserver/ldlogon) にマップし、SERVERCONFIG.EXE. (手順については、『System Manager ユーザーズ ガイド』の「デバイス エージェントのインストールと設定」の章にある「エージェントのプル」を参照) を実行します。
- 自己解凍型のデバイス インストール パッケージを作成します。このパッケージをローカル デバイス上で実行してエージェントをインストールします。この操作を実行するには、管理者権限でサーバにログインする必要があります。(手順については、『System Manager ユーザーズ ガイド』の「デバイス エージェントのインストールと設定」の章にある「インストール パッケージを使用したエージェントのインストール」を参照してください。)

エージェントをプッシュするには

1. [マイ デバイス] リストでターゲット デバイスを指定します (前述のデバイスを [マイ デバイス] リストに移動する手順を参照)。
2. 左側のナビゲーション ペインで [エージェントの構成] をクリックし、プッシュする構成を右クリックして [タスクのスケジュール] をクリックします。
3. 左側のペインで [ターゲット デバイス] をクリックし、[ターゲット一覧の追加] ボタンをクリックします。
4. [タスクのスケジュール] をクリックし、タスクをすぐに開始する場合は [すぐに開始] をクリックし、後で開始する場合は [後で開始] をクリックしてタスクの開始日と時刻を設定して、[保存] をクリックします。

タスクのステータスは [構成タスク] タブで表示できます。

Linux サーバ エージェントのインストール

Linux エージェントと RPM を Linux サーバ上にリモートで導入およびインストールできます。そのためには、Linux サーバを正しく設定する必要があります。Linux サーバを正しく構成する方法については、『*System Manager ユーザーズ ガイド*』の「デバイス エージェントのインストールと設定」の章にある「サーバ エージェントのインストール」を参照してください。

アラートの設定

デバイス上で問題またはその他のイベントが発生すると（デバイスのディスク領域の不足など）、System Manager
はアラートを送信します。これらのアラートは、アラートを呼び出す重要度レベルまたはしきい値を設定することで、カスタマイズできます。アラートをコンソールに送信し、特定のアクションを実行するようにアラートを設定できます。多数のイベントや潜在的な問題に対してもアラートを設定できます。製品には既定のアラートのルールセットが用意されています。この既定のルールセットは、監視コンポーネントをインストールするときに管理デバイスにインストールされます。.このアラートのルールセットは、ヘルス
ステータスのフィードバックをダッシュボードおよび
コンソールに提供します。この既定ルールセットには次のようなアラートが含まれます。

- ディスクが追加または削除された
- ディスク領域
- メモリ使用量
- 温度、ファン、電圧
- リモート コントロール アクティビティ
- パフォーマンス モニタ
- IPMI イベント（適用するハードウェア）

アラートについての詳細は、『System Manager ユーザーズ
ガイド』の「アラートの構成」の章を参照してください。

アラートの設定

デバイス上で問題またはその他のイベントが発生すると（デバイスのディスク領域の不足など）、System Manager
はアラートを送信します。これらのアラートは、アラートを呼び出す重要度レベルまたはしきい値を設定することで、カスタマイズできます。アラートをコンソールに送信し、特定のアクションを実行するようにアラートを設定できます。多数のイベントや潜在的な問題に対してもアラートを設定できます。製品には既定のアラートのルールセットが用意されています。この既定のルールセットは、監視コンポーネントをインストールするときに管理デバイスにインストールされます。.このアラートのルールセットは、ヘルス
ステータスのフィードバックをダッシュボードおよび
コンソールに提供します。この既定ルールセットには次のようなアラートが含まれます。

- ディスクが追加または削除された
- ディスク領域
- メモリ使用量
- 温度、ファン、電圧
- リモート コントロール アクティビティ
- パフォーマンス モニタ

アラートについての詳細は、『System Manager *ユーザーズ*
ガイド』の「アラートの構成」の章を参照してください。

ダッシュボードの実行

ダッシュボードには、使用しているデバイスのシンプルな概要が見やすく表示されています。ダッシュボードでは、各デバイスは色分けされたアイコンで表示され、アイコンの色によってデバイスの現在のヘルスがわかります。また、主要なトラブルシューティング ツールにすばやくアクセスすることもできます。

ダッシュボードを起動するには

- コア サーバで、[スタート]、[プログラム]、[LANDesk]、[LANDeskダッシュボード] の順にクリックします。.
- リモート ワークステーションのブラウザで、URLとして「http://coreserver/LDSM/db_frameset.asp」と入力します。
- コンソールで [ダッシュボード] をクリックします。

次の操作

これで、Server Manager を実行することができました。ここまでで使用した Server Manager の機能はほんのわずかで、しかもその機能の一部 (デバイス検索やエージェント構成など) しか活用していません。同梱のほかのガイド (『*インストールおよび導入ガイド*』および『*ユーザーズ ガイド*』) では、製品のすべての機能についてより詳細な情報が提供されています。一部の機能を以下に紹介します。

リモート コントロール： リモート ファイルにアクセスしたり、双方向でファイルを転送したり、リモート アプリケーションを実行したり、デバイスをリモートで再起動するなど、デバイスで起こる多数の問題をリモートで診断およびトラブルシューティングします。リモート セッション中は、ターゲット デバイスではなく使用しているコンピュータのキーボード レイアウトを使用し、そのリモート デバイスに対してあらゆる操作をすることが可能です。すべてのアクションがリモート デバイスでリアルタイムに実行されます。

ソフトウェア更新：
ネットワーク全体の管理デバイスに対して現行のパッチレベルのセキュリティを確立します。管理デバイス上で動作するさまざまなオペレーティング システムの脆弱性の評価、適切なパッチ実行可能ファイルのダウンロード、影響を受けるデバイスへの必要なパッチの導入およびインストールによる脆弱性の修正、パッチの正常インストールの確認を行って、現在の脆弱性情報を管理するための繰り返し手順を自動化できます。

アラート：
デバイスのいずれかが特定のしきい値に達した場合にアラートが送信します。監視機能に関連し、アラートはさまざまな方法で通知を送信できます。たとえば、デバイスのハード ドライブの使用率が 95% に達したときに通知する場合、アラートの送信方法を選択できます (電子メール、ポケットベル メッセージ、デバイスの再起動またはシャット ダウン、またはアラート ログへの情報追加など)。

クエリ： 特定のシステムまたはユーザ条件に基づいてコア データベースにあるデバイスを検索または整理することにより、ネットワークを管理します。管理デバイス

のリストに対してクエリを実行し、指定の条件 (本社にあるすべてのデバイス、または 256K の RAM を持つすべてのデバイスなど)
に一致するデバイスを検索してアクション別にグループ化できます。これらのグループは静的
(グループのメンバは手動でのみ変更できる) または動的
(メンバはデバイスが指定の条件に一致するか一致しないかにより変化する)
のいずれかに設定することが可能です。.

ソフトウェア配布 :ソフトウェア パッケージ (1 つ以上の MSI ファイル、実行可能ファイル、バッチ ファイル、RPM ファイル (Linux)、または LANDesk パッケージ ビルダによって作成されたパッケージ) をターゲット デバイスに配布するタスクを作成します。

監視 : サポートされている監視タイプ (ASIC の直接監視、インバンド IPMI、アウトオブバンド IPMI、および CIM など) のいずれかを使って、デバイスのヘルス
ステータスを監視します。監視によって、利用状況のレベル、OS
イベント、プロセスとサービス、パフォーマンスの履歴、およびハードウェア センサー
(ファン、電圧、温度など)
を含むデバイスに関するデータを追跡できます。アラートは監視エージェントを使ってアラート
アクションを開始する関連機能です。

レポート機能 :
ネットワーク上の管理デバイスに関する重要な情報を提供する、用途を特定したさまざまなレポートを生成できます。Server Manager では、コア
データベースにデバイスを追加し、これらのデバイスのハードウェアおよびソフトウェア
データを収集するためにインベントリ スキャン
ユーティリティを使用します。デバイスのインベントリ表示から取得したインベントリ
データは、表示および印刷できます。また、このインベントリ
データを使用してクエリを定義したり、デバイスをグループ化できます。レポート
ツールは、スキャンしたこのインベントリ データを収集し、見やすいレポート
フォーマットに整理することで、このデータを有効に活用します。これは、規制レポートのデータを収集およびフォーマットする場合に役立ちます。

非管理デバイス検索 :
コンソールによって管理されていないデバイスを検索します。検索は、新しいコンピュータを迅速に管理下にいれる最初のステップです。検索タスクをセットアップして、新しいコンピュータを毎月スキャンすることもできます。

ソフトウェア ライセンス監視 : ライセンスの準拠全体を追跡します。ソフトウェア
ライセンス監視エージェントは、データ
(デバイスにインストールされているすべてのアプリケーションについて、合計使用時間
(分)、起動回数、最後に起動した日付など)
を収集し、このデータをデバイスのレジストリに保存します。データは、製品の利用状況および拒否傾向を監視するために使用できます。エージェントは、最低限のネットワーク帯域を使用して、デバイス側の製品の利用状況を受動的に監視します。このエージェントは、モバイル
デバイスがネットワークに接続していなくても、利用状況を継続的に監視します。

OS 導入 : PXE ベースの導入ツールを使って、ネットワークのデバイスに OS
イメージを導入します。ハード ドライブが空のデバイスやオペレーティング

システムが使用できないデバイスに対して、イメージングを行うことができます。軽量 PXE
代表を使用すると、各サブネットに専用 PXE サーバを配置する必要がなくなります。OS
導入では、プロセスが開始されると、それ以降のエンド
ユーザまたは技術担当者による入力を必要とせずに新規デバイスの移行を効率よく行います。

*その他のブランドおよび名称は、それぞれの所有者に帰属します。

フェーズ 1 : 管理ドメインの設計

フェーズ 1 では、ネットワーク
インフラストラクチャに関する情報を収集し、管理ドメインをカスタマイズするための決定を行います。

このフェーズで説明する内容は次のとおりです。

ネットワーク情報の収集

ネットワークに関する重要な情報は System Manager
に関係するので、これを識別して収集します。特に、次の作業が重要です。

- デバイス構成の決定
- コア サーバの選択

コア サーバの選択

コア サーバは、管理ドメインの中心です。すべての主要なファイルおよびサービスは、コア
サーバに置かれます。物理的には新しいサーバでも用途を変更したサーバでもかもいません。

アラートの管理、コア データベースの照会、カスタム
スクリプトの作成などの管理作業を行う管理コンソールは、ブラウザから実行できます。

コア
サーバに選択したサーバがシステム要件を満たしていることを確認します。このフェーズの後にある「システム要件」を参照してください。

プログラム ファイルの配置計画

プログラム
ファイルのインストール先は、インストール時に指定できます。既定のインストール先ディレクトリを変更する特別な理由がない場合は、既定の場所を使用してください。インストール先ディレクトリを変更する場合は、インストール先ディレクトリのパスには 2 バイト文字は使用できません。

コア サーバ ファイルの既定のインストール先ディレクトリは次のとおりです。

C:¥Program Files¥LANDesk¥ManagementSuite

コア データベース

System Manager コア サーバに MSDE データベースをインストールします。各 MSDE データベースは、データベース サイズに 2 GB の制限があります。このデータベースがサポートするサーバの数は、ネットワークのインベントリ スキャン ファイル サイズに依存します。

5 つを超える並行処理をデータベースが行う場合は、MSDE に性能上の問題が発生することがあります。たとえば、5 人の System Manager 管理者が同時にデータベースにアクセスする場合です。

コア/クライアントのセキュリティ

本製品は証明書を使用した認証システムを使用しています。コアのインストール時に、セットアップによってそのコアの証明書が作成されます。クライアントはコアとの通信時にその証明書を検索します。コアに対する証明書を持っていないクライアントはそのコアとの通信を行いません。

デバイスは、信頼されている証明書ファイルが一致するコア サーバのみと通信します。各コア サーバは独自の証明書と秘密キーを持ち、既定で、各コア サーバから導入したクライアント エージェントは、ソフトウェアの導入元であるコア サーバとのみ通信します。

スコープの計画

役割ベース管理は、強力なセキュリティ管理機能です。コンソールの役割ベース管理ツールは、左ペインの [ユーザ] をクリックすることによってアクセスできます。管理者権限でログインしている必要があります。

役割ベース管理は、システムにユーザを追加して権限とスコープを割り当てることによって、高度なデバイス管理機能を提供します。権限は、ユーザに表示されるツールおよびユーザが使用できる機能を決定します (『Server Manager ユーザーズ ガイド』の第 1 章の「権限について」を参照してください)。スコープは、ユーザが管理できるデバイスの範囲を決定します (『Server Manager ユーザーズ ガイド』の「スコープの作成」を参照してください)。

ユーザの責任、ユーザに実行させる管理タスク、そしてユーザに表示、アクセス、および管理を許可するデバイスに基づいて役割を作成できます。デバイスへのアクセスは、国、地域、都道府県、市といった地理的な場所、あるいは特定のグループやサーバのタイプを基準にして制限できます。

このタイプの役割ベース管理を実装してネットワーク全体に適用するには、現在のユーザをセットアップするか、新しいユーザを作成して本製品のユーザとして追加し、必要に応じた (本製品の機能への) 権限と (管理デバイスへの) スコープを割り当てます。

コア サーバは、スコープを使用して、コンソール ユーザが認識できるデバイスを制限することができます。複数のスコープを 1 人のユーザに割り当てることができ、複数のユーザで同じスコープを使用できます。次の方法のいずれかを基本的なスコープにすることができます。

- (既定の) [すべてのコンピュータ] スコープ : ユーザがすべてのデバイスを表示できます。
- **クエリを基準**
  :ユーザは、管理者によって割り当てられた特定のクエリの選択された条件に一致するデバイスのみを認識できます。
- **グループを基準** :ユーザは、グループの基準に合ったデバイスを表示できます。

スコープの詳細については、『Server Managerユーザーズ ガイド』を参照してください。

システム要件

インストールする前に、次のシステム要件を満たしていることを確認してください。前提条件チェッカーが確認します。

コア サーバおよびデータベース サーバ

すべてのコア サーバおよびデータベース
サーバが概要にある次の要件を満たしていることを確認します。

- SP 4 が適用された Windows 2000 Server または Advanced Server、あるいは Windows Server 2003 Standard 版またはEnterprise 版 x86 SP1、または Windows 2000 R2
- Microsoft Data Access Components (MDAC) 2.8 以降
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- ASP.NET v1.1 スクリプト作成の IIS サポート
- Internet Explorer 6.0 SP1 以降
- Microsoft NT File System (NTFS)
- コア サーバとして使用する Windows サーバは、プライマリ ドメイン コントローラ (PDC)、バックアップ ドメイン コントローラ (BDC)、または Active Directory コントローラとしてではなく、スタンドアローン サーバとしてインストールする必要があります。
- SNMP がインストールされ、SNMP および SNMP トラップ サービスが開始される必要があります。
- 200 MB の容量がシステム ドライブで利用可能で、900 MB の容量が少なくとも 1 つのドライブで利用可能です。
- 管理者の権限
- LANDesk クライアントが正しいバージョンであるか、あるいはインストールされていない

コア サーバの要件
Windows のページファイルは、少なくとも 12 + *N* が必要です (ここで、*N* はコア サーバ上の RAM をメガバイトで表す数です)。この数値に満たない場合、アプリケーションはメモリ エラーを生成する場合があります。

同じコア サーバに Management Suite と Server Manager の両方の製品をインストールする場合には、そのコア コンピュータに 1 ギガバイトのメモリを搭載することを推奨します。

本製品のすべてのサービスを 1 台のサーバでホスト

小規模な管理ドメインの場合は、コア サーバおよびコア データベースを 1 台のサーバにインストールできます。これらのネットワークでは、一般的に保守が容易である既定の Microsoft MSDE データベースの使用を検討するものと考えられます。これは、System Manager の唯一のデータベース オプションです。

制限に関する検討事項

コアとデータベースをインストールするには、サーバが少なくともこれらのシステム要件を満たしている必要があります。

- Pentium 4 プロセッサ
- 10K RPM 以上の回転速度のドライブ上の 4 GB の空きディスク容量
- 768 MB 以上の RAM

管理サーバ コンピュータ

IT Management Suite では、サーバのオペレーティング システムとして次のものをサポートしています (すべてのオペレーティング システムを同等にサポートしているわけではありません)。

- Microsoft Windows 2000 Server (SP4)
- Microsoft Windows 2000 Advanced Server (SP4)
- Microsoft Windows 2000 Professional (SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server Standard Edition x86 (SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (SP1)
- Microsoft Windows XP Professional (SP2)
- Microsoft Windows XP Professional x64 (SP2)
- Windows Small Business Server 2000 (SP4)
- Windows Small Business Server 2003 (SP1)
- Red Hat Enterprise Linux v3 (ES) 32-bit – U6
- Red Hat Enterprise Linux v3 (ES) EM64t – U6
- Red Hat Enterprise Linux v3 WS 32-bit – U6
- Red Hat Enterprise Linux v3 WS EM64t – U6
- Red Hat Enterprise Linux v3 (AS) 32-bit – U6
- Red Hat Enterprise Linux v3 (AS) EM64t – U6
- Red Hat Enterprise Linux v4 (ES) 32-bit – U2
- Red Hat Enterprise Linux v4 (ES) EM64t – U2
- Red Hat Enterprise Linux v4 (AS) 32-bit – U2
- Red Hat Enterprise Linux v4 (AS) EM64t – U2
- Red Hat Enterprise Linux v4 WS 32-bit – U2
- Red Hat Enterprise Linux v4 WS EM64t – U2

- SUSE* Linux Server 9 ES 32-bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE* Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Linux 管理サーバ コンピュータ

以下は、Linux デバイスを管理するためのファイアウォールと RPM の前提条件の一覧です。

ファイアウォール

初めて管理エージェントをインストールし、コアと通信できるように Linux サーバを設定する場合には (「プッシュ」方法を使用)、SSH 接続が Linux サーバのローカル
ファイアウォールを通過することを許可する必要があります。

22 – TCP のみ

エージェントが (インベントリ スキャン、ソフトウェア配布、脆弱性更新などのために) コア
サーバと通信できるようにするには、Linux サーバのローカル
ファイアウォールが次のポート上で通信できるように設定する必要があります。

9593 – TCP のみ

9594 – TCP のみ

9595 – TCP と UDP の両方

管理エージェントと通信するには、Linux サーバのローカル
ファイアウォールが次のポート上で通信できるように設定される必要があります。

6780 – TCP のみ

必要な RPM (バージョン # 以降)

製品の RPM はすべて ...¥ManagementSuite¥ldlogon¥RPMS
ディレクトリに保存することをお勧めします。このディレクトリは http://core name/RPMS
で参照できます。

REDHAT_ENTERPRISE

python

RPM Version:2.2.3-5 (RH3)

2.3.4-14 (RH4)

Binary Version:2.2.3

pygtk2 RPM Version:1.99.16-8 (RH3)

2.4.0-1 (RH4)

Binary Version:

sudo

RPM Version:1.6.7p5-1

Binary Version:1.6.7.p5

bash RPM Version:2.05b-29 (RH3)

3.0-19.2 (RH4)

Binary Version:2.05b.0(1)-release

xinetd RPM Version:2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Binary Version:2.3.12

mozilla RPM Version:1.7.3-18.EL4 (RH4)

Binary Version:1.5

openssl RPM Version:0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Binary Version:0.9.7a

sysstat RPM Version:4.0.7-4

Binary Version:4.0.7

lm_sensors

RPM Version:2.6 (このバージョンは、新しい ASIC
コンピュータ上にセンサを表示するには十分でない可能性があります。詳細については、lm_sensors
ドキュメントか、あるいはウェブサイト (http://www2.lm-sensors.nu/~lm78) を参照してください。

SUSE LINUX

(SUSE 64)

bash

RPM Version:2.05b-305.6

mozilla

RPM Version: 1.6-74.14

net-snmp

RPM Version: 5.1-80.9

openssl

RPM Version:0.9.7d-15.13

python-gtk

RPM Version:2.0.0-215.1 [note:package name change]

python

RPM Version: 2.3.3-88.1

sudo

RPM Version:1.6.7p5-117.1

sysstat

RPM Version: 5.0.1-35.1

xinetd

RPM Version: 2.3.13-39.3

lm_sensors

RPM Version:NA (note:これは 2.6 バージョンのカーネルに含まれています)

製品のポートの使用

はじめに

ファイアウォール（またはトラフィックをフィルタするルータ）
のある環境で本製品を使用する場合、この製品が正しく機能するためには、ファイアウォールまたはルータの設定を調整する必要があります。このセクションでは、製品の各種コンポーネントによって使用されるポートについて説明します。ここで説明する内容は、ルータおよびファイアウォールを設定する際に必要になる情報で、各サブネット内でローカルにのみ使用するポートについての説明は除外します。

ファイアウォール規則の基礎知識

この情報はファイアウォール規則の設定に関するものです。ファイアウォール規則の設定という主題に馴染みがないユーザは、このセクションを読んで、主なコンセプトの基礎を理解してください。

ファイアウォール規則

「ポートを開く」というのは、正確な表現ではありません。単にファイアウォールに行って任意のポートを開くことはできません。ポートを開くとは、ファイアウォール規則を設定することを端的に示した表現です。ファイアウォール規則では、ファイアォールを通過することを許可するトラフィックと許可しないトラフィックを規定します。ファイアウォール規則は、ポート番号上のトラフィックをフィルタするだけではありません。規則は、プロトコル、発信元のポート番号と宛先のポート番号（インバウンド/アウトバウンド）、送信元の IP アドレスと送信先の IP アドレスなどに基づいて設定できます。

一般的なファイアウォール規則を以下に示します。「TCP ポート 9535 上の インバウンド
トラフィックを許可します。」本製品を使用するためには、リモート
コントロールをサポートするためにこの規則が必要になります。この規則は、次の 3
つの要素に基づきます。

1. プロトコル（TCP または UDP）
2. ポート番号
3. 方向（インバウンドまたはアウトバウンド）

ファイアウォール規則を設定するためには、これらの 3 つの要素が必須となります。

発信元と宛先ポート、および動的ポート

TCP または UDP 通信には、常に 2 つのポートが関係します。すべての TCP パケットまたは UDP パケットは、発信元ポートから宛先ポートに送られます。ファイアウォール規則は、発信元ポートまたは宛先ポート、あるいはその両方のポートに基づいて設定できます。このようにドキュメント内に一覧されるポートは、常に宛先ポートです。

5007（インベントリ サービスが使用）
などのよく知られたポートは、通信の片側のみを表します。通信のもう一方の側では、動的ポートを使用

します。動的ポートは、オペレーティング システムによって 1024 ～ 5000 の範囲に自動的に割り当てられます。

ファイアウォールと UDP トラフィック

TCP トラフィックがファイアウォールを通過することを許可するには (たとえば、ポート 5007 へのインバウンドの TCP 接続を許可するには)、ひとつの規則で十分です。TCP 接続を確立すると、データは双方向に接続を通過できます。

UDP トラフィックは、コネクションレスであるため、これとは異なります。たとえば、コアサーバは、既定で、タスクの開始前に UDP ポート 38293 でデバイスに対して「ping」します。ポート 38293 への送信 UDP パケットを許可するファイアウォール規則では、パケットはコアサーバからファイアウォールの外のデバイスにパケットを送ることができます。ただし、デバイスの応答パケットは送れません。

ポート 38293 への送信パケットと受信パケットの両方を許可するファイアウォール規則では、よく知られたポートを通信の片側のみがリッスンするため、どちらか一方の通信が動作しなくなります。もう一方の側の通信は動的ポートを使用します。コア サーバの送信パケットは動的ポートからポート 38293 に送られるため、デバイスの応答パケットは、ポート 38293 からポート 38293 でなく、同じ動的ポートに送られます。 両方向の通信を許可するには、発信元ポートまたは宛先ポートを 38293 に設定した UDP パケットを許可する規則が必要になります。このような規則は、すべての UDP ポートへのインバウンド パケットを許可するため、通常、イントラネットでは使用されますが、外部のファイアウォールでは使用されません。

こうした理由から、一般に UDP トラフィックは「ファイアウォールに適していない」とみなされます。もう一度先ほどの例を考えてみると、UDP ポート 38293 に代わってTCP ポート 9595 を使用できます。ファイアウォールを越えてデバイスを管理するときには、TCP ポートを使用するように製品を構成することを検討するはずです。

使用されるポート

ポート	方向	プロトコル	サービス
31770	コンソールからデバイスへ、デバイスからコアへ	TCP	コンソールとデバイス間の通信
6787	コンソールからデバイスへ	TCP	コンソールとデバイス間の通信

ポート	方向	プロトコル	サービス
9595	コンソールからデバイスへ	UDP	検索
9595	コンソールからデバイスへ	TCP	エージェント構成
623	コンソールからデバイスへ	UDP	ASF、IPMI 検索
9535	コンソールからデバイスへ	TCP	リモート コントロール

本製品でノードを管理するには、インストール済みの管理エージェントでノードを検索する必要があります。検索には、UDP ポート 9595
が使用されます。手動で個々のデバイスをコンソールに追加することもできますが、このためには、デバイスが UDP ポート 9595
の「ping」に応答する必要があります。コンソールとデバイスの間の通信は、TCP ポート 31770 と 6787
を使用します。後者のポート上のトラフィックは、HTTP ベースです。ASF (Alert Standard Forum)
検索の場合、UDP ポート 623 が使用されます。また、リモート コントロールについては、TCP ポート
9535 を使用します。IPMI 検索は、ASF 検索とリンクされていて、同じポート (UDP/623) を使用します。

フェーズ 2 : コア サーバのインストール

このフェーズでは、コア サーバのインストールについて説明します。

このフェーズで説明する内容は次のとおりです。

- コア サーバのインストール
- コア サーバのライセンス認証
- Windows デバイスへの導入
- Linux デバイスへの導入

このフェーズで概説するコンポーネントのインストールには、約 30 ～ 60 分かかります。

コア サーバのインストール

コア サーバをインストールするには

1. インストールを開始する前に、その他のアプリケーションを閉じて、開いているファイルを保存することをお勧めします。コア サーバとして選択した Windows 2000/2003 サーバで、次の手順を実行します。 製品メディアをドライブに挿入するか、インストール イメージから AUTORUN.EXE を実行します。[自動実行] 画面が表示されます。
2. [インストール要件をチェックしてインストール] をクリックします。
3. システム要件チェッカーが実行され、サーバが最小システム要件を満たしているかどうか検証します。すべての要件を満たしていることを確認します。満たされていない要件がある場合は、その要件のリンクの [失敗] をクリックし、失敗した要件のインストールに関するリンクや情報を表示します。
4. [今すぐインストール] をクリックしてセットアップ プログラムを実行します。
5. セットアップでインストールする言語を選択します。[**OK**] をクリックします。
6. [ようこそ] 画面が表示されます。[**次へ**] をクリックします。
7. [使用許諾契約] 画面で、条件に同意する場合は、[使用許諾契約を受け入れる] をクリックして操作を続行します。[**次へ**] をクリックします。
8. 既定のインストール先のフォルダを使用するか、または、カスタム インストール先フォルダを指定して、[次へ] をクリックします。インストール先フォルダ パスにはダブルバイト文字は使用できません。このフォルダを変更する場合は、製品マニュアルに記載されているパスに置き換えてください。
9. MSDE データベースのパスワードを入力します。このパスワードは後で必要になるため、[**次へ**] をクリックします。
10. コア サーバのセキュリティ証明書に対する組織および証明書の名前を入力します。この情報は名前を示し、証明書を説明します。[**次へ**] をクリックします。
11. [インストール準備完了] ページで、[インストール] をクリックします。製品のインストールが開始します。
12. セットアップが完了したら、[InstallShield ウィザード 完了] ダイアログが表示されます。

13. [完了] をクリックします。
14. セットアップにより、サーバの再起動が求められます。[はい] をクリックして、セットアップを終了します。サーバを再起動すると、インストールを完了するまで数分間セットアップが実行されます。最初の再起動時に、情報の入力は要求されません。

Windows 2003 Server に MSDE コア データベースをインストールする場合は、Windows がセットアップを妨害し、Setup.exe を開いてもいいかと尋ねる場合があります。この場合、[開く] をクリックしないと、製品が正しくインストールされません。
Intel Platform Extensions for LANDesk Software をインストールする場合には、Server Manager のインストール後に表示されるウィザードに従ってください。

コア サーバのライセンス認証

System Manager 製品をサーバ上で使用する前に、コア サーバのライセンス認証を行う必要があります。コア サーバのライセンス認証は、インターネットによって自動で行うことも、電子メールによって手動で行うことも可能です。ハードウェア構成を大幅に変更した場合は、コア サーバのライセンス認証を再度行う必要が生じる場合があります。

定期的に、コア サーバのライセンス認証コンポーネントが次の項目に関するデータを生成します。

- 使用しているデバイスの正確な数
- 個人を特定しない暗号化されたハードウェア構成
- 使用している特定の LANDesk Software プログラム (「サーバ カウント データ」と総称)

ライセンス認証によって、その他のデータが収集または生成されることはありません。ハード ディスクのサイズ、コンピュータの処理速度など、個人を特定しないハードウェア構成要素を使って、コア サーバ上でハードウェア キー コードが生成されます。ハードウェア キー コードは、暗号化されて LANDesk に送信され、暗号化に使われるプライベート キーはコア サーバ上にのみ保存されます。その後で、ハードウェア キー コードが LANDesk Software によって使用され、認可された証明書の一部を作成します。

コア サーバをインストールした後で、コア サーバ使用開始ユーティリティ ([スタート]、[すべてのプログラム]、[LANDesk]、[コア サーバの使用開始]) が最初の起動時に実行して、OEM 先が提供したユーザ名とパスワードを

コア サーバ使用開始ユーティリティを使うと、System Manager を Server Manager または Management Suite にアップグレードできます。「Management Suite または Server Manager と System Manager の使用方法」を参照してください。

認証を終えてコア サーバがアクティブになると、コンソールの [プリファレンス] メニューの [ライセンス] を選択して、製品のライセンス情報を表示できます。インテルの OEM ライセンスでは、すべてのインテル ブランドのサーバまたはメイン ボード上で製品のエージェントを実行することが可能です。

コア サーバの使用開始 ユーティリティについて

コア
サーバの使用開始ユーティリティを使って、新規サーバの使用開始時にそのサーバを認証することができます。[スタート]、[プログラム]、[LANDesk]、[コア サーバの使用開始]
の順にクリックし、ユーティリティを起動します。コア
サーバがインターネットに接続していない場合は、このセクションの「手動によるコア
サーバのライセンス認証とサーバ カウント データの確認」を参照してください。

各コア サーバは、そのコア サーバに固有の認可された証明書を持つ必要があります。

定期的に、コア サーバは「¥Program Files¥LANDesk¥Authorization
Files¥LANDesk.usage」ファイルを生成してライセンス情報を検証します。このファイルは、定期的に
LANDesk Software ライセンス サーバに送信されます。このファイルは XML
形式で、電子署名が済んでおり、暗号化されています。このファイルに手動で変更を加えると、ファイルの内容と LANDesk Software ライセンス サーバに対する次の利用状況レポートが無効になります。

コア サーバは、HTTP で LANDesk Software ライセンス サーバと交信します。プロキシ
サーバを使用している場合は、ユーティリティの [**プロキシ**]
タブをクリックし、プロキシ情報を入力します。コア
サーバがインターネットに接続している場合、ライセンス
サーバとの交信は自動で行われ、ユーザの操作は必要ありません。

コア サーバの使用開始
ユーティリティは、ダイアルアップによるインターネット接続を自動で起動しません。ダイアルアップ接続を手動で起動してライセンス認証ユーティリティを実行した場合は、ライセンス認証ユーティリティはダイアルアップ接続を使用して利用状況のレポートを送信することができます。

コア サーバがインターネットに接続していない場合は、このセクション内で後でふれるようにサーバ
カウントを手動で検証して送信することができます。

コア サーバのライセンス認証

サーバのライセンスを認証するには

1. [スタート]、[プログラム]、[LANDesk]、[コア サーバの使用開始] の順にクリックします。
2. [**LANDesk ユーザ名とパスワードを使ってこのコア サーバのライセンスを認証する**]
   をクリックします。

このユーザ名とパスワードは自動的に入力されます。

手動によるコア サーバのライセンス認証とサーバ カウント データの確認

コア サーバがインターネットに接続していない場合は、コア サーバの使用開始ユーティリティはサーバ
カウント データを送信できません。ライセンス認証とサーバ

カウント検証データの送信を電子メールを使って実行するよう求めるメッセージが表示されます。電子メールによるライセンス認証は、簡単で時間のかからない処理です。コア
サーバ上で手動によるライセンス認証の実行を求めるメッセージが表示されたり、または コア
サーバの使用開始
ユーティリティを使用していて手動によるライセンス認証を求めるメッセージが表示されたりする場合は、次の手順に従います。

手動によりコア サーバのライセンス認証とサーバ カウント データの確認を行うには

1. コア サーバがノード カウント データを手動で検証するように求める場合は、「¥Program Files¥LANDesk¥Authorization Files」フォルダに activate.txt というデータ
   ファイルが作成されます。このファイルを電子メール メッセージに添付し、licensing@landesk.com へ電子メールで送信してください。メッセージの件名や本文は空白のままで問題ありません。
2. LANDesk Software がメッセージの添付ファイルを処理し、メッセージが送信されたメール
   アドレスに返信されます。LANDesk Software
   メッセージに新しいライセンス認証ファイルが添付され、その処理手順が本文に記されます。
3. 添付されているライセンス認証ファイルを ¥Program Files¥LANDesk¥Authorization Files
   フォルダに保存します。コア
   サーバがすぐにこのファイルを処理し、ライセンス認証ステータスを更新します。

手動によるライセンス認証に失敗したり、コア
サーバが添付されたライセンス認証ファイルを処理できない場合は、ライセンス認証ファイルは .rejected という拡張子が追加され、Windows のイベント ビューアにあるアプリケーション
ログによりユーティリティが詳細な情報を記録します。

コンソールへのログイン

セットアップが完了し、コア サーバを再起動してコア
サーバのライセンスが認証されたら、ブラウザを開いて、以下の形式のサーバのアドレスを入力して、コンソールを起動します。http://servername/ldsm。(コア
サーバで、[スタート]、[すべてのプログラム]、[LANDesk]、[System Manager] をクリックします。)
コンソールを起動すると、コンソールのログイン ウィンドウが表示されます。ログインするために、LDSM をインストールしたアカウントの資格情報の入力を要求するプロンプトが表示されます。ログオンできるのは、コア サーバの LANDesk Management Suite
グループのメンバだけです。既定では、コアをインストールしたときにログインに使用したユーザが LANDesk Management Suite
グループに追加されます。他のユーザがコンソールにアクセスできるようにする場合は、このグループにユーザを追加します。

ブラウザで初めてコンソールを起動する場合、コンソールの表示に 90
秒ほどかかることがあります。この遅れは、サーバがコードの一部を 1
回だけコンパイルするためです。コンソールは 2 回目以降はすばやく起動します。

Windows デバイスへの導入

本製品では、スケジュールされたプッシュを使用した設定方法をサポートしているので、エージェントをリモート導入できます。

まだ 標準の管理エージェントを実行していない Windows 2000/2003
サーバのプッシュを使用した設定を有効にするには、次のように適切なログイン資格を入力する必要があります。

1. コア サーバで [スタート]、[プログラム]、[LANDesk]、[LANDesk Configure Services] の順にクリックしてから [スケジューラ] タブをクリックします。
2. [ログインの変更] をクリックします。
3. [ユーザ名とパスワード] フィールドに、ドメイン管理者アカウントを domain¥username 形式で指定します。
4. スケジューラ サービスを停止して再起動します。
5. Web コンソールから目的のデバイスをターゲットにして、[エージェントの構成]、[スケジュールされているタスク] の順にクリックして構成を導入します。

コア サーバと同じドメインに属している Windows 2000/2003
メンバを設定するときに、ドメイン管理者を指定できます。他のドメインで Windows 2000/2003
サーバを設定するには、信頼関係をセットアップする必要があります。上記のステップ 3
で指定したアカウントは、スケジューラ サービスをコア
サーバで実行するときに使用するアカウントでもあることに注意してください。アカウントに**サービスとしてログオンする**権限があることを確認してください。

プッシュ設定に失敗し、「エージェントを検出できません」というメッセージが表示された場合は、次の手順を実行して問題を特定してください。これらの手順では、プッシュ設定時のスケジューラの動作を再現しています。

1. スケジューラ サービスの実行に使用しているユーザ名を検出します。
2. コア サーバで、ステップ 1 で検出したユーザ名を使用してログインします。
3. ドライブを ¥¥server name¥C$ にマップします。失敗の可能性が最も大きいのがこのステップです。失敗には 2 つの理由が考えられます。サーバの管理者権限を持っていないか、または、このユーザに管理者権限がない場合は、サーバの管理共有フォルダ (C$) が無効になっているためです。
4. ¥¥server name¥C$¥$ldtemp$ ディレクトリを作成し、このディレクトリにファイルをコピーします。
5. Windows サービス マネージャを使用し、サーバでサービスを開始して停止してみます。

1. IPMI 対応デバイスでは、BMC パスワードを入力する必要があります。[サービスの設定] の [BMC パスワード] タブを使用して IPMI Baseboard Management Controller (BMC) のパスワードを作成します。 [BMC パスワード] タブで、[パスワード] テキスト ボックスにパスワードを入力し、[パスワードの確認入力] テキスト ボックスにパスワードを再入力して、[OK] をクリックします。

パスワードは英数字で 15 文字以内にします。使用できる文字は 0～9 の数字、または a～z の大文字または小文字のアルファベットです。

Intel* AMT 対応デバイスの場合、Intel AMT パスワードを入力する必要があります。[サービスの設定] の [Intel AMT 構成] タブを使用して、Intel Active Management Technology 対応デバイスのパスワードを作成または変更します。

Intel AMT のパスワードを設定するには

1. [Intel AMT 構成] タブで現在のユーザ名とパスワードを入力します。このユーザ名とパスワードは Intel AMT 構成画面で設定されているものに一致する必要があります (コンピュータの BIOS 設定からアクセスできます)。
2. ユーザ名とパスワードを変更するには、[新しい Intel AMT パスワード] セクションで設定してください。
3. [**OK**] をクリックします。この変更は、そのクライアント設定の実行中に行います。

注意：
新しいパスワードは堅牢なパスワード、つまり次の条件を満たしたパスワードである必要があります。

- 7 文字以上
- アルファベット文字、数字、および記号を含む
- 2 番目から 6 番目の文字のうち、少なくとも 1 文字が記号である
- 前のパスワードと大幅に異なる
- 名前やユーザ名を含まない
- 一般的な単語や名前ではない

Linux デバイスへの導入

Linux エージェントと RPM を Linux サーバ上にリモートで導入およびインストールできます。そのためには、Linux サーバを正しく設定する必要があります。Linux サーバにエージェントをインストールするには、ルート権限が必要です。

既定の Linux のインストール (Red Hat 3 と 4、および SUSE) には、Linux 標準エージェントに必要な RPM が含まれています。[エージェントの構成] で監視エージェントを選択する場合は、追加 RPM、sysstat が必要です。

最初の Linux エージェント構成では、コア サーバは SSH を使用してターゲット Linux サーバに接続します。認証されたユーザ名とパスワードで SSH 接続を確立しておく必要があります。この製品は、公開キーと秘密キーによる認証をサポートしていません。コア サーバと Linux サーバ間のすべてのファイアウォールで SSH ポートを許可する必要があります。コア サーバからの SSH 接続をサードパーティ製 SSH アプリケーションでテストすることを検討してください。

Linux エージェントのインストール パッケージには、シェル スクリプト、エージェントの tarball、.INI エージェント構成、およびエージェントの認証証明書が含まれています。これらのファイルは、コア サーバの LDLogon 共有フォルダに格納されます。シェル スクリプトは、tarball からファイルを抽出して RPM をインストールし、エージェントの構成で指定した間隔でエージェントのロードとインベントリ スキャナを実行するようにサーバを設定します。ファイルは /usr/landesk に配置されます。

コア サーバ上のスケジューラ サービスを、Linux サーバ上の SSH 認証資格情報 (ユーザ名とパスワード) を使用するように設定する必要もあります。スケジューラ サービスは、これらの資格情報を使用してサーバにエージェントをインストールします。サービス設定ユーティリティを使用して、スケジューラ サービスで代替の資格情報として使用する SSH 資格情報を入力します。このユーティリティが完了すると、スケジューラ サービスを再起動するように要求されます。再起動を要求されない場合は、[スケジューラ] タブで [停止] をクリックしてから [開始] をクリックして、サービスを再起動します。これにより、変更が反映されます。

Linux サーバを設定してコア サーバに Linux 資格情報を追加したら、Linux エージェントを導入できるように、[マイ デバイス] リストにサーバを追加する必要があります。サーバにエージェントを導入するには、そのサーバを [マイ デバイス] リストに追加しておく必要があります。そのためには、[デバイス検索] で Linux サーバを検索します。

Linux サーバを検索するには

1. [デバイス検索] で、各 Linux サーバの検索ジョブを作成します。標準のネットワーク スキャンを使用して、検索する範囲の開始 IP と終了 IP に Linux サーバの IP アドレスを入力します。多数の Linux サーバがある場合は、IP アドレスの範囲を入力します。検索する IP 範囲を追加したら、[OK] をクリックします。
2. 作成した検索タスクをクリックし、[スケジュール] をクリックすることによって、そのタスクをスケジュールします。タスクが終了したら、管理する Linux サーバが検索プロセスで検出されているか確認します。
3. [デバイス検索] で、管理するサーバを選択し、[ターゲット] をクリックしてこのデバイスを [ターゲット] リストに追加します。ウィンドウの下半分にある [管理] タブをクリックします。[選択されたデバイスを移動します] をクリックして [移動] をクリックします。これにより、[マイ デバイス] リストにサーバが追加されるので、導入先のサーバとして選択できるようになります。

Linux エージェント構成を作成するには

1. [エージェントの構成] で、[新規] をクリックします。
2. 構成名を入力して [HP-UX] または [Linux Server Edition] をクリックし、[OK] をクリックします。
3. 作成した構成を選択し、[編集] をクリックします。
4. エージェントを選択します。
5. [インベントリ] タブで、オプションとスキャナの実行間隔を選択します。インストール スクリプトによって、選択した間隔でスキャナを実行する cron ジョブが追加されます。
6. [変更内容の保存] をクリックします。

エージェント構成を導入するには、[エージェントの構成] で構成を選択して [タスクのスケジュール] をクリックします。[構成タスク] で、タスクを構成してタスクの進捗状況を監視します。

注意：インベントリ スキャナがインストール後に最初のスキャンを完了するまでは、Linux コンピュータのヘルス情報は取得できません。 **Linux エージェント構成をプルするには**

1. Linux コンピュータに一時ディレクトリを作成して (/tmp/ldcfg など)、次をそのディレクトリにコピーします。
    1. LDLOGON¥unix¥linux ディレクトリのすべてのファイル。
    2. 構成に基づいて名づけられたシェル スクリプト (<構成名>.sh) を一時ディレクトリにコピーします。
    3. 構成に基づいて名づけられた *.0 ファイルを一時ディレクトリにコピーします。* は、8 つの文字を表します (0-9、a-f)。
    4. <構成名>.ini
       ファイルに一覧表示されているすべてのファイルを一時ディレクトリにコピーします。これらのファイルを特定するには、「FILExx」という INI ファイルを探します。「xx」は数字です。検索される大部分の項目は、手順 1 コピーされていますが、.XML ファイルはコピーする必要があります。ファイル名は変更できませんが、次の例外があります。
        - alertrules¥<任意のテキスト>.ruleset.xml は、internal.ruleset.xml に名称変更する必要があります。
        - monitorrules¥<任意のテキスト>.ruleset.monitor.xml は、masterconfig.ruleset.monitor.xml に名称変更する必要があります。
2. コンピュータが IPMI/BMC コンピュータ (インストレーションに監視機能も含まれている) の場合、次の行をコマンド ラインに入力します。

```
export BMCPW="(bmc password)"
```

3. ルートとして実行し、構成のシェル スクリプトを実行します。たとえば、スクリプトの名前が「pull」の場合、以下に使用されているフルパスを使用します。

```
/tmp/ldcfg/pull.sh
```

4. 一時ディレクトリとその中のファイルをすべて削除します。

注意： エージェントを Linux コンピュータに対してプッシュまたはプルし、

```
./linuxuninstall.sh -f ALL
```

を実行してクリーンしてから再度プッシュまたはプルする場合、操作の完了後に唯一コンピュータ上に残っているのは、GUID を持つファイルのみです。

-f オプションにより、製品のすべてのディレクトリが削除されます。詳細については、Linux のアンインストール ドキュメントを参照してください。

フェーズ 3 : 段階的な導入

フェーズ 3
では、導入について段階ごとに説明します。「導入」とは、管理ドメインに含めるデバイスに管理機能を拡張するプロセスです。

デバイスに製品エージェントおよびサービスをロードすることで、本製品の導入を行います。これにより、ワークステーションやサーバを 1 か所から管理できるようになります。

この章では以下の内容を説明します。

段階的導入計画

段階的導入は次の 3 つの原則に基づいています。

1. 利用頻度が低いか既存のネットワークに与える影響が小さなコンポーネントから、利用頻度が高いか影響が大きなコンポーネントの順にデバイスへ導入します。
2. より多くのエージェントを導入する前に、各管理デバイスの機能が安定していることを確認します。
3. 本製品の導入は、必要なトラブルシューティングを複雑にする可能性のある、一度にすべてのデバイス
   タイプにエージェントを導入する方法ではなく、綿密な計画に基づいたフェーズによって行います。

フェーズ 1 ～ 2
を完了すると、デバイスに本製品を導入するこの最終フェーズを開始する準備が整います。

デバイス設定のためのチェックリスト

デバイスを設定するために Web
コンソールからリモートにエージェントを導入するか、あるいは管理デバイスからエージェントをインストールできます。プッシュ ベースの設定を実行するには、すべての IPMI または Intel* AMT
コンピュータのサービスを設定しておく必要があります。Configure Services アプレットを使用して、コアサーバおよびデータベースについて、次のサービスを設定できます。Configure Services
アプレットを起動するには、コア サーバ上で [スタート]、[プログラム ファイル]、[LANDesk]、[LANDesk Configure Services] の順にクリックします。[BMC パスワード] または [Intel AMT 構成]
タブを使用します。

- **プッシュを使用した設定**：
  エージェントの構成を使用して、デバイス設定を定義します。[サービスの設定] から Intel AMT または IPMI コンピュータに必要な資格を入力します（『ユーザーズ ガイド』の「サービスの設定」を参照してください）。目的のデバイスをターゲットにして、そのデバイスに構成をプッシュするタスクをスケジュールします。詳細については、『ユーザーズ ガイド』の「エージェントの構成」を参照してください。
- **手動設定**：管理デバイスからコア サーバの LDLogon 共有フォルダにドライブをマップし、SERVERCONFIG.EXE サーバ コンフィグレーション プログラムを実行します。デバイスに導入するコンポーネントを対話形式で選択する必要があります。

大規模な環境ではインストールと設定を行うデバイスの数が多いため、手動設定は現実的ではありません。多くの場合、管理デバイスにエージェントをプッシュすることになります。製品インストールではコアにエージェントが自動ではインストールされないことに注意してください。コアにエージェントをインストールしてから、手動でコアを再起動する必要があります。

デバイスの設定方法にかかわらず、コンソールの [エージェントの構成] を使用して導入するデバイス構成を作成したことを確認してください。

Windows XP Professional SP2 または 2003 SP1 システムでは、製品が完全に機能するためには、ファイアウォールを手動で構成する必要があります。これらのデバイスに対して次の設定を指定してください。 **管理サーバ**：

ファイルとプリンタの共有 – TCP 139、445、UDP 137、138
（この設定をしないとエージェントのプッシュが機能しません）

ソフトウェアの配布 – TCP 9594、9595（この設定をしないとエージェントのプッシュが機能しません）

詳細設定 – ICMP – [エコー要求の着信を許可する]
（この設定が有効でないとデバイスが検出されません）

コア サーバ：

インベントリ – 5007

管理デバイス上でこれらの設定を行うには、[スタート]、[コントロール パネル]、[セキュリティ センター] の順にクリックします。本製品は、次を含む既定のエージェント構成になっています。標準の管理エージェント、ソフトウェア更新、監視エージェント。

インストールするコンポーネントのみを含む新しい構成を作成するか、または（OEM バージョンの場合のみ）既定のエージェント構成に Intel Active System Console を追加できます。エージェントの導入プロセスが累積的ではないことに注意してください。導入を行うと、既存のエージェントがすべてアンインストールされます。構成に新しいエージェントを追加するには、その構成に必要な以前のエージェントすべてに新しいエージェントを含める必要があります。

デバイス構成を作成するには

1. 左側のナビゲーション ペインで、[エージェントの構成] をクリックします。

2. [**新規**] をクリックします。
3. [構成名] ボックスに新しい構成の名前を入力します。

「DBServer」や「Executive Office
Server」など、作成する構成の説明になるような名前を入力します。既存の名前または新しい名前を指定できます。

4. [Linux server edition] または [Microsoft Windows server edition] または [HP-UX] を選択します。
5. 製品ソフトウェアのエージェントをインストールしないで IPMI
対応のサーバを管理するには、設定が IPMI 対応サーバ用である場合は、[IPMI BMC のみの構成] を選択して、[OK] をクリックします。。
6. 作成した構成を選択し、[編集] をクリックします。

各種タブのいくつかのオプションには、選択した構成に対して適用可能ではないため、淡色表示されていることがあります。たとえば、[IPMI BMC-only Windows configuration]
を選択する場合、設定可能なオプションはありません。

7. [エージェント] タブで、導入するエージェントを選択します。
    - **すべて** : 選択したサーバにすべてのエージェントをインストールします。
    - **ソフトウェア更新** :
      ソフトウェア更新エージェントをインストールします。このエージェントをインストールすると、利用可能な更新を検出するスキャナの実行方法を設定できます。
    - **監視** :
      選択したデバイスに監視エージェントをインストールします。監視エージェントは、ASIC の直接監視、インバンド IPMI、アウトオブバンド IPMI、Intel Active System Console、Intel AMT および CIM などの多くのタイプの監視に対応しています。
8. [構成] は情報目的でのみ表示されます。
9. 再起動オプションを選択します。

手動による再起動とは、選択したエージェントが再起動を要求した場合でも、デバイスが再起動しないことを意味します。デバイスを手動で再起動する必要があります。デバイスが再起動が必要な場合は、デバイスが再起動するまでインストールしたエージェントは正しく機能しません。必要に応じてデバイスを再起動するサーバは、選択したエージェントで再起動が必要な場合にのみデバイスを再起動します。

注意 : 既存の 8.5 エージェントを更新するデバイスのみ、再起動が必要です。

10. [インベントリ] タブで、インベントリ
スキャナ構成の設定を指定します。これらの設定について次に説明します。

- **自動更新** : ソフトウェア スキャン中にリモート デバイスがコア サーバからソフトウェア リストを読み取ります。このオプションが設定されている場合、デバイスがソフトウェア リストにアクセスできるように、各デバイスのドライブをコア サーバの LDLOGON ディレクトリにマップする必要があります。ソフトウェア
リストへの変更は、デバイスに直ちに適用できます。

- **手動更新**：ソフトウェア スキャン中にタイトルを除外するために使用されるソフトウェア リストが各リモート デバイスにダウンロードされます。ソフトウェア リストがコンソールから変更されるたびに、リモート デバイスにソフトウェア リストを手動で送信する必要があります。
- **インベントリ スキャナ設定**：インベントリ スキャナが実行する時間です。頻度を選択したり、スタートアップ時に実行するように指定できます。

インベントリ スキャナの [実行時間範囲を指定] オプションを選択すると、スキャナの実行が可能な時間の範囲を指定できます。デバイスが指定した時間内にログインすると、インベントリ スキャンが自動的に実行されます。デバイスがすでにログインしている場合は、開始時間が来ると、インベントリ スキャンが自動的に開始されます。このオプションは、一度にすべてのデバイスにスキャンを送信するのではなく、段階的にインベントリ スキャンを実行する場合に便利です。

- **スタートアップ時に実行する**：インベントリ スキャナは、デバイスが起動するたびに実行します。

11. [ルールセット] タブで、構成に含める任意の監視またはアラート ルールセットを選択します。これらのルールセットは、ldlogon/alertrules フォルダに保存されています。新しいルールセットは、[監視] または [アラート] に作成できます。新しく作成したルールセットをドロップダウン リストに表示するには、カスタム ルールセットの XML を生成する必要があります。
12. [変更内容の保存] をクリックしてエージェントの設定を保存します。

デバイスへの導入の詳細については、この章の後半の「エージェント構成アーキテクチャについて」を参照してください。

Windows デバイスへの導入

本製品では、スケジュールされたプッシュを使用した設定方法をサポートしているので、エージェントをリモート導入できます。

まだ 標準の管理エージェントを実行していない Windows 2000/2003 サーバのプッシュを使用した設定を有効にするには、次のように適切なログイン資格を入力する必要があります。

1. コア サーバで [スタート]、[プログラム]、[LANDesk]、[LANDesk Configure Services] の順にクリックしてから [スケジューラ] タブをクリックします。
2. [ログインの変更] をクリックします。
3. [ユーザ名とパスワード] フィールドに、ドメイン管理者アカウントを domain¥username 形式で指定します。
4. スケジューラ サービスを停止して再起動します。
5. Web コンソールから目的のデバイスをターゲットにして、[エージェントの構成]、[スケジュールされているタスク] の順にクリックして構成を導入します。

コア サーバと同じドメインに属している Windows 2000/2003
メンバを設定するときに、ドメイン管理者を指定できます。他のドメインで Windows 2000/2003
サーバを設定するには、信頼関係をセットアップする必要があります。上記のステップ 3
で指定したアカウントは、スケジューラ サービスをコア
サーバで実行するときに使用するアカウントでもあることに注意してください。アカウントに**サービスとしてログオンする**権限があることを確認してください。

プッシュ設定に失敗し、「エージェントを検出できません」というメッセージが表示された場合は、次の手順を実行して問題を特定してください。これらの手順では、プッシュ設定時のスケジューラの動作を再現しています。

1. スケジューラ サービスの実行に使用しているユーザ名を検出します。
2. コア サーバで、ステップ 1 で検出したユーザ名を使用してログインします。
3. ドライブを ¥¥server name¥C$
   にマップします。失敗の可能性が最も大きいのがこのステップです。失敗には 2
   つの理由が考えられます。サーバの管理者権限を持っていないか、または、このユーザに管理者権限がない場合は、サーバの管理共有フォルダ (C$) が無効になっているためです。
4. ¥¥server name¥C$¥$ldtemp$ ディレクトリを作成し、このディレクトリにファイルをコピーします。
5. Windows サービス マネージャを使用し、サーバでサービスを開始して停止してみます。

1. IPMI 対応デバイスでは、BMC パスワードを入力する必要があります。[サービスの設定] の
   [BMC パスワード] タブを使用して IPMI Baseboard Management Controller (BMC)
   のパスワードを作成します。 [BMC パスワード] タブで、[パスワード] テキスト
   ボックスにパスワードを入力し、[パスワードの確認入力] テキスト
   ボックスにパスワードを再入力して、[OK] をクリックします。

パスワードは英数字で 15 文字以内にします。使用できる文字は 0～9 の数字、または a～z
の大文字または小文字のアルファベットです。

Intel* AMT 対応デバイスの場合、Intel AMT パスワードを入力する必要があります。[サービスの設定]
の [Intel AMT 構成] タブを使用して、Intel Active Management Technology
対応デバイスのパスワードを作成または変更します。

Intel AMT のパスワードを設定するには

1. [Intel AMT 構成]
   タブで現在のユーザ名とパスワードを入力します。このユーザ名とパスワードは Intel AMT
   構成画面で設定されているものに一致する必要があります (コンピュータの BIOS
   設定からアクセスできます)。
2. ユーザ名とパスワードを変更するには、[新しい Intel AMT パスワード]
   セクションで設定してください。
3. [**OK**] をクリックします。この変更は、そのクライアント設定の実行中に行います。

注意：
新しいパスワードは堅牢なパスワード、つまり次の条件を満たしたパスワードである必要があります。

- 7 文字以上

- アルファベット文字、数字、および記号を含む
- 2 番目から 6 番目の文字のうち、少なくとも 1 文字が記号である
- 前のパスワードと大幅に異なる
- 名前やユーザ名を含まない
- 一般的な単語や名前ではない

エージェントの正常な導入の確認

管理エージェントがデバイスに正常に導入されたかどうかを確認するには、コンソール内から次のタスクが実行可能であることを確認します。これらのタスクを実行するための詳細については、『System Manager ユーザーズ ガイド』の各機能に対応する章を参照してください。

インベントリ

- [マイ デバイス]
  リストで、デバイスをダブルクリックして、インストールされているエージェントのリストを表示します。
- インベントリ クエリを実行します。
- デバイスを選択し [インベントリ] をクリックしてデバイスのデータを表示します。
- Windows デバイスの WIN.INI ファイルを変更し、デバイスを再スキャンしてその変更が CHANGES.LOG に記録されたことを確認します。

コマンド ラインからのデバイス導入

SERVERCONFIG.EXE をコマンドライン
パラメータと使用して、デバイスにインストールされているコンポーネントを制御できます。

SERVERCONFIG.EXE はスタンドアローン モードで起動できます。これは、コア サーバの (システム ドライブ) ¥Program Files¥LANDesk¥ManagementSuite¥LDLogon にあります。SERVERCONFIG.EXE は Windows 2000/2003 サーバから読み込み可能な ¥¥coreservername¥LDLogon
共有フォルダでも表示できます。

エージェント構成アーキテクチャについて

SERVERCONFIG.EXE について

SERVERCONFIG.EXE は、製品の設定ユーティリティです。SERVERCONFIG.EXE は、次の 3 つのステップで、Windows サーバを管理できるように設定します。

1. SERVERCONFIG は、別の LANDesk
   製品でコンピュータが設定されているかどうかを調べます。設定されている場合は、古いファイルを削除して他の変更を取り消します。

2. SERVERCONFIG は、サーバの設定または再設定が必要かどうかを決定するために CCDRIVER.TXT という隠しファイルを探します。SERVERCONFIG が実行する決定プロセスについては、次のセクションで説明します。デバイスの設定または再設定が必要でない場合は、SERVERCONFIG が終了します。
3. デバイスの設定または再設定が必要な場合は、SERVERCONFIG が適切な初期化ファイル (SERVERCONFIG.INI) を読み込み、そのファイルに含まれている命令を実行します。

SERVERCONFIG.EXE を 2 回実行し、最初の実行時とは異なるエージェントを選択する場合、最初の実行時のエージェントは削除されます。以前エージェントをインストールしている場合でも、SERVERCONFIG.EXE を新たに実行するごとに、必要な各エージェントを選択する必要があります。

SERVERCONFIG.EXE には、次のコマンドライン パラメータを使用できます。

パラメータ	説明
/I=	含めるコンポーネント (引用符が含まれる) : "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" これらのパラメータは同一コマンド ライン上で結合できます。 例 : SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	IP を使用して設定します。
/L または /Log=	デバイスが設定されたか設定されなかったかを記録する CFG_YES および CFG_NO ログ ファイルへのパスです。
/LOGON	[LOGON] という接頭辞が付いたコマンドを実行します。
/N または /NOUI	ユーザ インターフェイスを表示しません。
/NOREBOOT	終了時にデバイスを再起動しません。
/P	実行するためのユーザ アクセス許可を要求します。
/REBOOT	実行後に強制的に再起動します。

/TCPIP	IP と同じです (「/IP」を参照)。
/X=	除外するコンポーネント。 例 : SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= 既定の SERVERCONFIG.INI ファイルの代わりに使用するデバイス構成ファイルを指定します。 たとえば、NTTEST.INI という設定ファイルを作成した場合は、次の構文を使用します。 SERVERCONFIG.EXE /CONFIG=TEST.INI カスタム .INI ファイルは SERVERCONFIG.EXE と同じディレクトリに存在する必要があります。また、/config パラメータでは、接頭辞 95 を付けないファイル名を使用することに注意してください。
/? または /H	ヘルプ メニューを表示します。

標準の管理エージェントの導入

標準の管理エージェントはほとんどのコンポーネントで必要であり、本製品の基本となるプロトコルです。

脆弱性スキャナの導入

脆弱性スキャナ エージェントは、スキャンと修復操作の両方を実行します。[セキュリティ
タスクのスケジュール] ボタンで、パラメータを使用しないで vulscan.exe
を起動するタスクを作成します。パラメータを使用しないで起動する場合、vulscan は、レジストリ キー
“hklm¥software¥intel¥landesk¥LDWM”、値 “CoreServer” にアクセスして、コア
サーバの場所を見つけます。次に、スキャンする最新の脆弱性情報のリストを要求し、スキャンを実行して、結果をコア サーバに送信します。スキャン結果は、[検出された更新]
リストに保存されます。検出された更新はコアにダウンロードする必要があります。修正プロセスによって更新にパッチを当てることが可能です。修正プロセスによって 1
つ以上のパッチが正常にインストールされると、再スキャンが行われ、新しいスキャン結果がコアに送信されます。これは LANDesk の更新および OEM の更新用です。

インベントリ スキャナの導入

インベントリ スキャナを使用して、コア
データベースにデバイスを追加したり、デバイスのハードウェアおよびソフトウェア
データを収集したりできます。インベントリ
スキャナはデバイスが初期設定されると自動的に実行されます。スキャナはハードウェアおよびソフトウェア データを収集し、コア
データベースに入力します。その後、デバイスが起動されるたびにハードウェア
スキャンが実行されますが、ソフトウェア スキャンはユーザが指定した間隔で実行されます。

監視エージェントの導入

監視エージェントは、ASIC の直接監視、インバンド IPMI、アウトオブバンド IPMI、Intel AMT、および CIM などの多くのタイプの監視に対応しています。

Active System Console の導入

System Manager のインターフェイスまたはメニューを通して Intel Active System Console
にアクセスできるようにするエージェントをインストールします。このエージェントはインテル製ボードのあるデバイスにのみインストールされ、非インテル製ボードへの導入にこのエージェントを含めてもインストールされません。

コア サーバのアンインストール

コンポーネントを導入する際に特定の方法に従う必要があるのと同様に、コンポーネントをアンインストールする際にも対応する方法に従う必要があります。

次のセクションに各コンポーネントの正しいアンインストール方法を示します。次の順序でコンポーネントをアンインストールする必要があります。

1. デバイスから製品エージェントをアンインストールします。
2. コア サーバをアンインストールします。

デバイスから製品エージェントをアンインストールする

ネットワークから製品ソフトウェアをアンインストールする際の最初のステップは、デバイスからのエージェントのアンインストールです。

エージェントをサーバからアンインストールするには

1. 管理者権限のあるアカウントでサーバにログインします。
2. コア サーバの ManagementSuite 共有フォルダにドライブをマップします。
3. コマンド プロンプトを開き、ManagementSuite
   フォルダのドライブ文字を変更してから、次のように入力します。

uninstallwinclient.exe

4. アンインストールは自動的に実行され、すべてのエージェントが削除されます。

[スタート] メニューにある [ファイル名を指定して実行]
を選択し、「¥¥*コア名*¥LANDesk¥ManagementSuite¥uninstallwinclient.exe」を指定して実行することもできます。**Linux サーバから Linux エージェントを完全に削除するには**

1. ManagementSuite 共有フォルダで linuxuninstall.tar.gz ファイルを探し、[Linux]
   ボックスにコピーします。
2. x、z、および f
   オプションを使ってこのファイルを実行します。コマンドラインは次のようになります。

tar xzf linuxuninstall.tar.gz

3. ファイルの実行後、コマンドラインから ./linuxuninstall.sh を実行します。

このファイルのヘルプは、-h オプションで実行すれば表示されます。 注意： エージェントを Linux コンピュータに対してプッシュまたはプルし、

./linuxuninstall.sh -f ALL

を実行してクリーンにしてから再度プッシュまたはプルする場合、コンピュータの GUID が削除されるため、同じ名前と IP を持つ同じコンピュータの重複したデータベースエントリが作成されることに注意してください。

–f オプションにより、製品のすべてのディレクトリが削除されます。詳細については、Linux のアンインストール ドキュメントを参照してください。

アンインストール後に残るのは、/etc/ldiscnux.conf ファイルのみです。このファイルは、データベースが重複デバイスで乱雑にならないように、そこに残されます。このデバイスをデータベースに戻す予定がない場合、このファイルも安全に削除できます。UninstallWinClient.exe は ManagementSuite 共有フォルダにあります。この共有フォルダにアクセスできるのは、管理者のみです。このプログラムは、このプログラムを実行しているデバイスの製品エージェントをアンインストールします。これは、インターフェイスを表示しないで、非表示で実行する Windows アプリケーションです。削除したデータベースでサーバの 2 つのインスタンスを表示できます。これらのインスタンスの 1 つには、履歴データのみが含まれ、もう 1 つのインスタンスには、転送されるデータが含まれます。

注意 : Uninstallwinclient.exe は、エージェントのアンインストール後に既定でデバイスを再起動します。再起動しないようにするには、コマンドラインに /noreboot スイッチを追加します。

コア サーバのアンインストール

ネットワークから本製品をアンインストールする最後のステップとして、コア サーバ上でソフトウェアをアンインストールします。それを行う前に、サーバから製品ソフトウェア エージェントがアンインストールされていることを確認します。

コア サーバをアンインストールするには

1. コア サーバに行きます。
2. [スタート]、[設定]、[コントロール パネル] の順にクリックし、[プログラムの追加と削除] をダブルクリックします。
3. インストールされている場合、[Intel Platform Extensions for LANDesk software] を選択して、[追加と削除] をクリックします。
4. 本製品のソフトウェアをアンインストールするには、[LANDesk ソフトウェア] を選択します。
5. [**追加と削除**] をクリックします。

コア データベースのアンインストール
コア データベースは手動でアンインストールする必要があります。

データベースのアンインストール

既定では、LANDesk® System Manager のアンインストール時にコア データベースはアンインストールされません。重要 :LANDesk® System Manager

をコンピュータに後で再度インストールする場合は、コア
データベースをアンインストールしないでください。

コア データベースをアンインストールするには

1. コア サーバに行きます。
2. [スタート]、[設定]、[コントロール パネル] の順にクリックし、[プログラムの追加と削除] をダブルクリックします。
3. コア データベースをアンインストールするには、[Microsoft SQL Server Desktop Engine (LDMSDATA)] を選択します。
4. [**追加と削除**] をクリックします。

データベース ファイル
Microsoft SQL Server Desktop Engine を削除しても、LANDesk® System Manager が使うデータベース ファイルは削除されません。データベースをコンピュータに残しても、ディスク領域を使用する以外は問題ありません。手動でこれらのデータベース ファイルを削除するには、¥ProgramFiles¥Microsoft SQL Server¥MSSQL$LDMSDATA¥Data フォルダのコンテンツを削除します。

サポート

Web で LANDesk Software のオンライン サポート サービスを利用できます (英語のみ)。サービスには LANDesk Software
製品に関する最新情報が含まれています。インストールの注意点、トラブルシューティングのヒント、ソフトウェアのアップデート、カスタマ サポート情報などもあります。次の Web
サイトを開いて、本製品のページにアクセスします。

http://www.landesk.com/support/index.php

リリース
ノートおよびマニュアルの最新版をダウンロードすることもできるので、製品の出荷時に入手できなかった情報が得られます。OEM 製造元から System Manager を受け取った場合には、OEM
製造元のサポート サービスにご連絡ください。

本書または Web サイトの LANDesk Software サポートを参照しても問題が解決できない場合、LANDesk Software では有料サポート、コンサルタント、およびパートナー
サービスを提供しています。詳細については、次のカスタマ サポートのページを参照してください。

http://www.landesk.com/wheretobuy/

カスタマ サポートに連絡する際は、次の情報をご準備ください。

- お客様の氏名、会社名、使用している製品のバージョン
- お客様が使用しているネットワーク オペレーティング システムの名前とバージョン
- インストールしたパッチまたはサービス パック
- 問題を再現する詳細手順
- 問題を解決するために既に行った手順
- 使用しているデータベース アプリケーションの種類、インストールしているビデオ
  カードのブランド、使用しているコンピュータのメーカーおよびモデルなど、お客様のシステムに固有の情報がカスタマ サポートの技術者にとって問題の理解に役立ちます。