

インテル® クラウド・ビルダーズ・ガイド： インテル® Xeon® プロセッサ搭載 プラットフォームにおける クラウドの設計と導入

Enomaly Elastic Computing Platform* Service Provider Edition

ホワイトペーパー

インテル® クラウド・
ビルダーズ・ガイド

Enomaly Elastic
Computing Platform*



対象読者と目的

クラウド・コンピューティングは、データセンター事業者（サービス・プロバイダーやホスティング事業者など）および一般企業にとって、拡張性の向上とコスト削減への道を開きます。こうした目標を達成できる新しいクラウド・インフラストラクチャーを確立するためには、経験が必要となります。インテルは、インテル® クラウド・ビルダーズ・プログラムを通じて主要クラウドベンダーと協力し、顧客がクラウド・インフラストラクチャーを容易に設計、導入、および管理できるよう支援します。

インテル® クラウド・ビルダーズ・プログラムは、クラウド導入の出発点として、基本的なハードウェア計画と、Enomaly Elastic Computing Platform* Service Provider Edition などの利用可能なクラウド・ソフトウェア管理ソリューションを提供します。本資料で説明するユースケースは、特定の顧客のニーズに合わせてより複雑な利用モデルや導入モデルを構築する際に、ベースラインとして使用できます。

本資料は、顧客や社内ユーザーへのクラウド・コンピューティング・サービスの提供によって、既存のデータセンター・インフラストラクチャーを活用することで、一定の収益増を実現しようとしているクラウド・サービス・プロバイダー、クラウド・ホスティング事業者、および企業の IT 部門を対象としています。



目次

概要	3	複数のユーザーによる VM の複製	12
はじめに	4	ネットワークの分離	12
設計原則	4	VM の構成管理	13
ECP の論理アーキテクチャー構成	5	複数のユーザーの課金	13
Enomaly ECP SPE 実装の概要	5	新しいサーバーの追加	13
Enomaly の ECP 製品	5	サービスのスケールアップとスケールダウン	13
拡張性のある設計	6	障害シナリオ	14
Enomaly ECP のコマンドおよび制御アーキテクチャー	6	サービスのシャットダウン	14
テストベッドの計画の概要	7	観察と分析	14
ハードウェアの説明	7	環境のストレステスト	14
物理アーキテクチャー	7	障害モードの検証	14
システム設計	7	パフォーマンスの検証	15
技術レビュー	8	次のステップ	15
インストールの概要	8	考慮事項	16
ユースケースの詳細	9	拡張性	16
アクター	9	ネットワーク・テクノロジー・アーキテクチャー	16
ユースケースの概要	9	ストレージ・アーキテクチャー	16
実行と結果	9	ハードウェアに関する考慮事項	16
セットアップとソフトウェアの検証	9	ソリッドステート・ドライブ (SSD)	16
使用する仮想マシンイメージの作成	10	セキュリティに関する考慮事項	16
ユーザーの作成	10	追加情報	17
複数のユーザーによるサービス・インスタンスの作成	11	用語集	17
サービスの監視	11	リファレンス	17

概要

その機敏性によるメリットとコスト削減によって、クラウドの概念と原理には大きな関心が集まっています。近年、多くの企業が公共のインターネット経由でアクセスできるクラウド・インフラストラクチャーを構築しており、現在は、顧客がアプリケーションをホストするために利用できるサービスを提供しています。代表的なクラウドサービスは、Infrastructure as a Service (IaaS)、Platform as a Service (PaaS)、および Software as a Service (SaaS) に分類できます。

既存のワークロード、組織固有のワークロード、および組織の厳格なコントロールが必要とされるワークロードでは、IaaS 構造を使用することが最良の選択といえます。IaaS クラウドサービスをサポートおよびホストする場合、収益を生み出すための顧客向けサービス（パブリッククラウド）であるか、企業のファイアウォールの内側にある組織内サービス（プライベート・クラウド）であるかにかかわらず、まず最初に問題となるのは、そのクラウドを構築するための手順です。

選択肢、トレードオフ、および決定事項が多数存在する点を考慮するならば、まずは、熟知した環境を出発点とし、その上にクラウドを構築できることが何より重要となります。このレポートでは、インテル® Xeon® プロセッサ 5500 番台と、Enomaly Elastic Computing Platform* (ECP) Service Provider Edition (SPE) を利用してクラウドを構築するための一連の作業の概要を示します。

ここで紹介するクラウド実装は、インテル® Xeon® プロセッサ 5500 番台を搭載した 5 台のサーバーで構成されます。これらのサーバーは、サービスとして公開されます。Enomaly ECP SPE は、サーバープールとストレージプールを区別しないため、クラウドを構築および管理するための非常に簡単なメカニズムが提供されます。本資料では、Enomaly ECP SPE を使用することでマルチテナンシーをどのようにサポートできるのかという点に注目します。マルチテナンシーのサポートにより、ストレージおよびネットワークを分離するとともに、インフラストラクチャーは、異なる「顧客」に属する仮想マシン (VM) をホストすることが可能になります。Enomaly ECP SPE は、非常に強力でありながらシンプルなポータル・インターフェイスを提供します。このインターフェイスを使用することで、ストレージが接続された IaaS をいかに容易に構築できるかを示していきます。

このリファレンス・デザインは、複数台のサーバーによる 1 つの“クラスター”と単一のストレージプールによって構成されます。理論的には、Enomaly ECP SPE を使用してプロビジョニングできる仮想マシンの数に上限はありません。Enomaly ECP SPE は、ここで実装したものよりも複雑なアーキテクチャーで、数千のサーバーから成る非常に大規模なクラウドをサポートできます。エンドユーザーのリソース要件に応じて、サーバーごとに許可する仮想マシンの数を必要に応じて定義できます。今回のリファレンス・デザインでのクラウドの設定では、5 つのノードで合計 160GB のメモリーを使用します。VMM (ハイパーバイザー) が約 500MB を占有するため、環境内の 5 つのサーバーノードで最大 $5 \times 31 = 155$ の VM をサポートし、各 VM に 1GB のメモリーを割り当てることができます。より軽量なコンピューティング・リソースのクラウド構成を設計する場合は、各仮想マシンに 1GB 未満のメモリーを割り当てるなど、目的に応じたカスタマイズが可能です。

Enomaly ECP SPE のポータル・インターフェイス（現在のどのブラウザからでもアクセス可能）を使用することで、ここでは複数の「顧客」の仮想マシンのプロビジョニングを可能にしています。また、リモート・デスクトップ・プロトコル (RDP) や仮想ネットワーク・コンピューティング (VNC) などのリモート接続プロトコルを使用して、これらのマシンに接続することも可能となります。各「顧客」のトラフィックは、VLAN パケットタグを使用して他のすべての「顧客」から分離されます。このケース固有のクラウド構成では、ネットワーク・ファイル・システム (NFS) を使用して、仮想イメージ・リポジトリのストレージを提供しました。仮想マシンの各インスタンスは、その仮想マシンが実行されているノードのローカルディスクに存在します。NFS を選択したのは、使いやすく導入も簡単であるという理由からです。稼働本番環境の並列構成またはクラスター構成では、より堅牢なストレージ・アーキテクチャーを使用することをお勧めします。検討すべき選択肢として、GFS (主要 Linux* ディストリビューションで提供され、Red Hat Inc. がサポート) などのクラスター・ファイル・システム・ソリューションがあります。これは、多数のベンダーの iSCSI ストレージやファイバーチャネル SAN ストレージと組み合わせることができます。クラウド導入の規模によっては、NAS テクノロジーを基盤とする、より軽量なソリューションや、高パフォーマンスのネットワーク・リンクまたは結合されたネットワーク・リンクで補完された、よりシンプルなサーバーベースのストレージ・ソリューションも検討対象となります。

ネットワーク・トラフィックは、仮想化された Enomaly ECP SPE ノードによって管理されます。システムのボトルネックとなる要素の 1 つに、ネットワーク・トラフィックのスループットがあります。テストベッドでは、クラウド・コンピューティング環境の増加する帯域幅のニーズに対処するために、10GB イーサネットを使用しました。Enomaly ECP Manager Agents と Enomaly ECP Node Agents は、インテル® Xeon® プロセッサ 5500 番台を搭載したサーバーに実装されました。

インテル® Xeon® プロセッサ 5600 番台を搭載したサーバーは、単位面積当たりの電力性能に優れているため、高密度のクラウド・アーキテクチャーに最も適しています。また、インテル® Xeon® プロセッサ 5600 番台を搭載したプラットフォームは、単位面積当たりの電力消費の最適化を支援する、インテル® インテリジェント・パワー・ノード・マネージャーなどの電力管理機能も備えています。

インテル® Xeon® プロセッサ 5600 番台は、インテル® Xeon® プロセッサ 5500 番台よりも性能が最大 60% 向上し¹、消費電力が最大 30% 削減されます。² また、新しいセキュリティー機能として、データ暗号化を高速化するインテル® Advanced Encryption Standard-New Instructions (インテル® AES-NI) と、仮想化環境で仮想マシンの起動前に悪意のあるソフトウェアが挿入されるのを防ぐ、インテル® トラストッド・エグゼキューション・テクノロジー³ (インテル® TXT) も搭載しています。

はじめに

設計原則

使用した基本的な設計原則は、初期費用と運用費用を最適化しながら、信頼性のあるデータの分離によるマルチテナンシー、拡張性、および柔軟性に対応するクラウド・アーキテクチャーの実装を提供することです。

インフラストラクチャーの運用コストを最小限に抑えるために、接続を統一したサーバーおよびストレージの同種のプールを使用し、管理、トラブルシューティング、およびキャパシティの追加や削除をできる限り簡単に行えるようにしました。ただし、これは、クラウドに含まれるサーバー要素またはストレージ要素が 1 種類に限られるという意味ではありません。次世代のサーバー・テクノロジーが利用可能になった場合などに備え、今後新しいプールを追加できるように、あえて統一されたサーバー、ストレージ、およびネットワークのプールを作成するよう努めました。この設計手法により、ワークロードの配置の自動化、外部ネットワークおよびストレージの接続、クラウド内でのワークロード管理の委任が可能になります。

仮想化によって拡張が可能になり、新しいハードウェアを追加することなく、突然のワークロード変更に対処するために必要な柔軟性がもたらされます。パブリッククラウド環境では、ユーザー間でデータおよびワークロードを確実に分離できるように、設計には細心の注意を払う必要があります。これに対して、企業では、分離を確保するための適度な制御は必要ですが、一部のアクセス制限が緩和されます。

最後に、クラウドのすべてのコンポーネント（サーバー、ネットワーク、ストレージなど）において、障害の発生を想定しておく必要があります。アプリケーションまたはクラウド管理ソフトウェアは、障害発生時に必要な復旧アクションを実行できなければなりません。各コンピューティング要素の状態を共有ストレージに保持するか、障害が発生したデバイスに対してアクションを再試行する責任をアプリケーションが負わなければなりません。企業の標準的なクラウド非対応のワークロードの場合、アプリケーションを仮想マシンにラップし、対応するす

べてのデータを共有ストレージに格納する必要があります。こうすることで、サーバーで障害が発生したときに、クラウド管理ソフトウェアは別のサーバーへの仮想マシンの移行や、別のサーバー上での仮想マシンの再起動を簡単に実行できます。

この実装を構築する際に考慮した、設計上の留意点は次のとおりです。

- 標準のインテル® サーバー・ビルディング・ブロックを使用しているため、ラック内の任意のサーバーを任意の目的に使用できます。この構成では、「特別な」サーバーも特別な接続もありません。すべてのサーバーは物理的に同じ方法で構成されます。これにより、ワークロードを簡単に再配置または再割り当てすることができ、プロビジョニング時にワークロードの構成を簡単に自動化できます。
- フラットなレイヤー 2 ネットワークにより、実装コストを削減し、任意のワークロードを任意のサーバーに割り当てる柔軟性を維持できます。小規模なクラウドの場合、この手法は柔軟性がありますが、サーバー数が多い大規模なデータセンター・レベルでは、ボトルネックが発生する可能性があります。Enomaly ECP SPE は、さらに高度なネットワーク・トポロジーをサポートしていますが、このテストベッドには必要ありませんでした。
- サーバーのワークロードを分離するために、Xen* Hypervisor を使用しました。また、ネットワーク・トラフィックは、ネットワーク・パケット・タグ (VLAN) とルーティングを使用して、Enomaly ECP SPE によって分離しました。Xen* は、KVM や VMware* に加えて、Enomaly ECP SPE がサポートするハイパーバイザーの 1 つです。
- クラスターからアクセスできるストレージを提供する低コストの便利な方法として、NFS サーバーと Direct Attached Storage (DAS) を併用しました。Enomaly ECP SPE は、クラスター・ファイル・システムや SAN などの高度なストレージ・アーキテクチャーの使用もサポートしているため、ノードのローカルストレージを使用しなくて済みます。

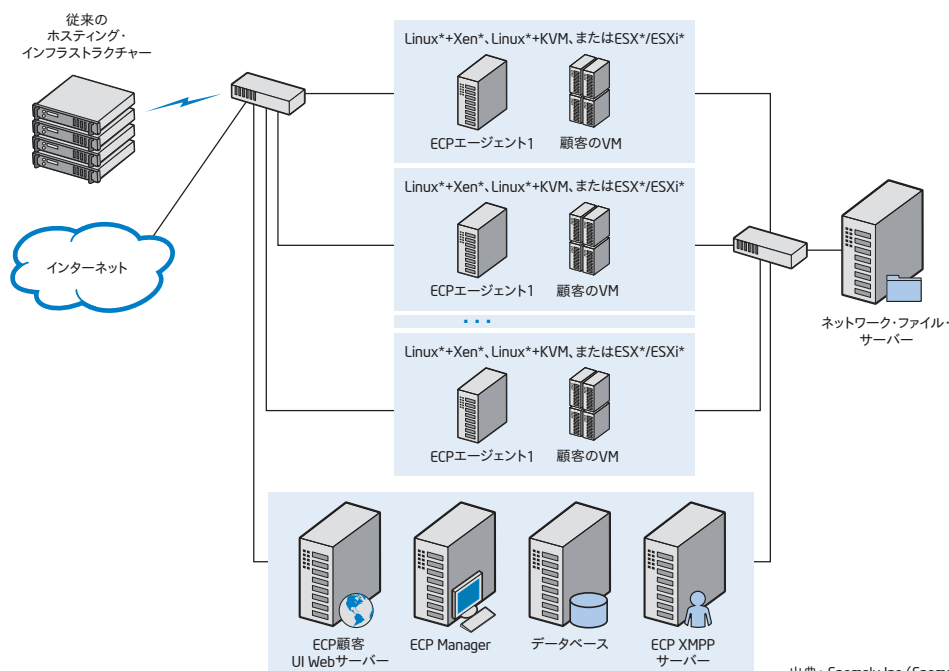


図 1. Enomaly ECP SPE の基本的な導入アーキテクチャー

ECP の論理アーキテクチャー構成

図 1 は、このハードウェア設計で使用した Enomaly ECP SPE [1] 導入の論理アーキテクチャーを示しています。これは、小規模なテストベッドに適した Enomaly ECP SPE 導入の基本的なアーキテクチャーです。本資料で使用されている手法は、共通ストレージプールとアクセスポイントにアクセスできるサーバープールの作成です。

図 2 は、Enomaly ECP SPE がサポートする、より高度な論理アーキテクチャーを示しています。これは参考のために用意されたものであり、テストベッドでは使用しませんでした。

Enomaly ECP SPE 実装の概要

Enomaly の ECP 製品

Enomaly の ECP Service Provider Edition は、柔軟性と高い経済性を兼ね備えた強力なクラウド・コンピューティングの提供を目指しているサービス・プロバイダーにとって、1つの解決策となります。

Enomaly ECP Service Provider Edition

Enomaly の SPE 製品は、高度に分化した強力な機能セットを備えた、完全な「Cloud in a Box (パッケージ化されたクラウド)」ソリューションです。この製品は、収益を生み出すオンデマンドのインフラストラクチャー・クラウド・コンピューティング・サービスを、顧客に対して迅速かつ容易に提供したいと考えている通信事業者、サービス・プロバイダー、およびホスティング事業者の要件を満たすことを目的としています。

ECP SPE の機能は次のとおりです。

- マルチテナントのキャリアクラスの完全なクラウド・サービス・プラットフォーム
- 詳細なリソース測定機能と課金機能

- シンプルでありながら強力な顧客セルフサービス・ポータル (ブランド化と国際化に対応)
- 顧客のワークロードに対応する HA 機能
- 強力なセキュリティ機能 (Enomaly ECP High Assurance Edition では、追加の High Assurance (高信頼性) 機能セットも提供)
- スケールアップおよびスケールアウト機能
- ホット・スペア・サーバーの瞬時起動
- パブリック VLAN とプライベート VLAN (顧客ごと) によるセキュリティ
- アプリケーション・マーケットプレースの統合: サービス・プロバイダーは、事前に構築されたクラウド・アプリケーションを ECP App Center から顧客に直接公開し、無料または有料で提供できます。既存のシステムイメージのこのライブラリーには、ビジネス・アプリケーションとインフラストラクチャー・コンポーネント (負荷分散装置やファイアウォールなど) の両方が含まれており、顧客はこのライブラリーからクラウド上で VM を直接プロビジョニングできます。詳細およびスクリーンショットについては、<http://www.enomaly.com/Cloud-Service-Pr.cloudhosting.0.html> (英語) を参照してください。

Enomaly Elastic Computing Platform* (ECP) は、サービス・プロバイダーまたは企業のクラウド・コンピューティング・プラットフォームを構成するソフトウェア製品です。

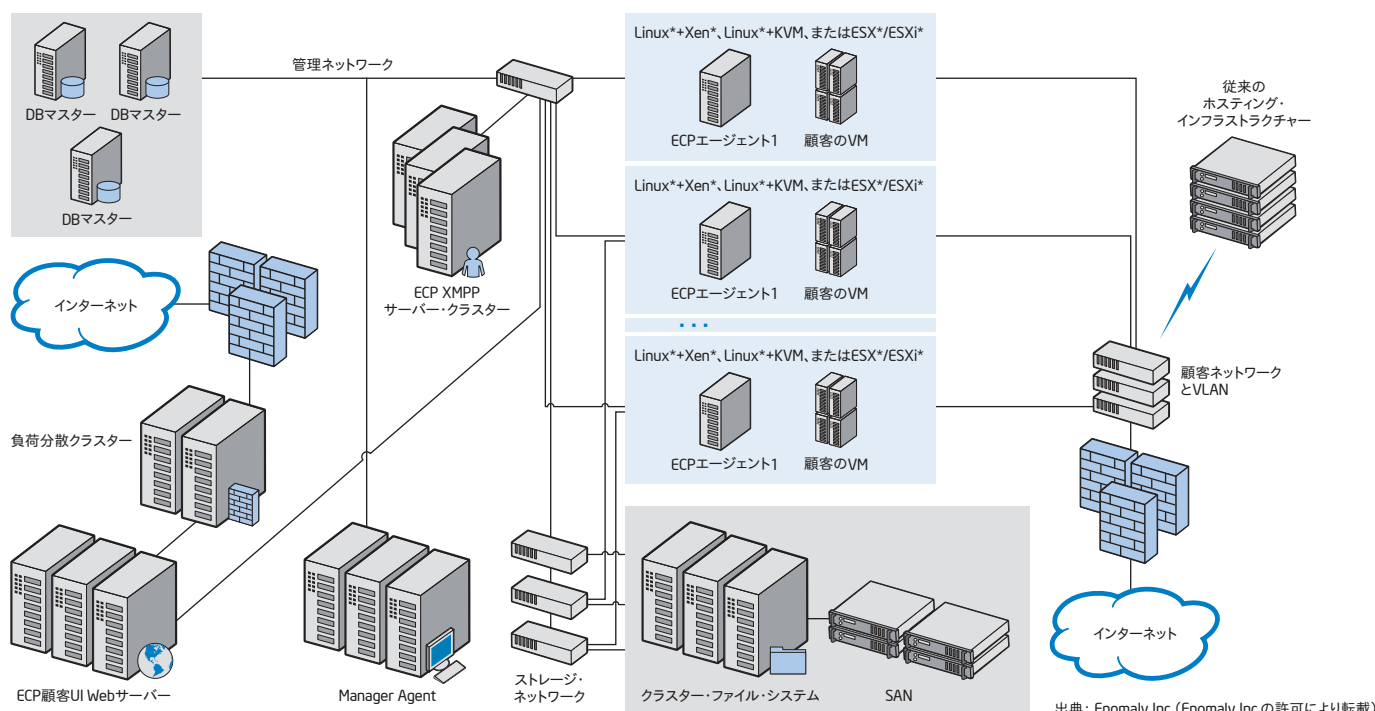


図 2. Enomaly ECP Service Provider Edition のキャリアグレードの導入アーキテクチャー

- 強力な自動化 API (顧客向け API と管理 API)
- ワークロードのインテリジェントで動的なプロビジョニングおよびオーケストレーション
- 課金システム、プロビジョニング・システム、および運用監視システムとの柔軟性のある統合
- Enomaly の堅牢なプロビジョニング・エンジンおよびオーケストレーション・エンジンを利用可能。以前のオープン・ソース・バージョンは、世界中の 15,000 の組織が既に導入済み

ECP のアーキテクチャーの原理と設計理念

Enomaly ECP [2] [3] は、通信事業者またはサービス・プロバイダー (ホスティング企業など) が IaaS サービスを顧客に提供できるようにするための、完全なエンドツーエンドのプラットフォームです。Enomaly ECP は、堅牢な分散型アーキテクチャーを基盤としています。ECP は、インターネット・クラウドの主要属性をサービス・プロバイダーのデータセンターに適用します。インターネットと同様に、Enomaly ECP では分散型コマンド / 制御構造モデルを使用するため、重大な障害が発生した場合にも稼働し続けることができます。ECP のシステム・アーキテクチャーは、最適レベルのフォールトトレランス、アプリケーションの下位 / 上位互換性、拡張性、信頼性、保水性、可用性、保守性、有用性、およびセキュリティを実現します。

拡張性のある設計

モジュール式で組み合わせ可能

ECP は、モジュール式の組み合わせ可能な多数のコンポーネントから構成されます。ユーザーが特定のアプリケーションのための仮想アーキテクチャーを設計すると、その仮想アーキテクチャーは、アプリケーションから要求されるモジュールを実行し、相互接続することによって展開されます。そのため、ECP はさまざまなアプリケーションの導入において効率的に運用できます。

分散化

一元的に調整されることなく、複数の冗長性のあるコンポーネントが相互運用されるインターネット自体のアーキテクチャー上でパターン化されたアーキテクチャーを通じて、ECP は高レベルの信頼性と大規模な拡張を実現します。

1,000 ノードでも、100,000 ノードや 100 万ノードの規模でも有効に運用できる拡張性のあるクラウド・プラットフォームを構築するには、疎結合の分散型アーキテクチャーを活用することが不可欠となります。クラウドは、1 人の人間または 1 つの組織が管理するのではなく、分散化された有機的組織体のように動作しなければなりません。インターネットと同様に、中央当局を置くことなく日々の処理の 99% を調整できる必要があります。このように管理されたクラウドに導入されるアプリケーションは、単一障害ポイントが減少または排除されるため、適応性とフォールトトレランスが向上します。

オーバーサブスクリプション

コスト効率を高めるために、キャリアクラスの IaaS プラットフォームでは、合意済みの最小限のサービス標準を提供しながら、使用量がピークに達する期間と使用量が少ない期間の両方で、リソースを効率的にプロビジョニングできる必要があります。

Enomaly の ECP では、オーバーサブスクリプションと Class-Of-Service ベースのリソース割り当て管理という、2 つの必須の原則に基づいてこの課題に取り組んでいます。これらにより、強力なキャパシティ制御が可能になります。パブリック・クラウド・インフラストラクチャーでは、オーバーサブスクリプション・モデルは、ピーク時の最大使用レベルへのリソース割り当て率、ピーク時の使用頻度と使用量、および最小限のサービスレベル合意によって異なります。重要なのは、顧客ごとに特定のサービス品質を保証しながら、同時に通常使用量のベンチマークの標準偏差近辺でリソースを管理することです。

Enomaly ECP の割り当てシステムでは、全顧客にサービスを提供する指定のリソースプール全体にわたり、あらかじめ定められたレベルの偏差を管理します。サービス・プロバイダーは、(故意または不注意による) 過度の使用や誤用から保護された状態を維持しながら、各自の環境をオーバーサブスクライブできます。さらに、利用層、サービス品質層、および追加リソースを要求どおりに動的にプロビジョニングする機能が組み込まれたモデルを使用して、さまざまな価格体系とコスト体系を実装できます。

異種リソースへの統一的アクセス

Enomaly ECP が提供する統一的アクセスメカニズムは、複数の仮想サーバー・プラットフォーム、複数のハイパーバイザー、複数のデータセンターにまたがる可能性がある多数の計算ノードなど、異種リソースの集まりの共通管理ポイントを提供します。ECP のすべてのインターフェイス (管理ユーザー・インターフェイス、完全にブランド化可能な顧客セルフサービス・インターフェイス、およびエンドユーザー / 管理 ReST API) で、地理的に離れた複数の場所に分散するさまざまなリソースを同時に管理できます。

Enomaly ECP のコマンドおよび制御アーキテクチャー

ECP は、各計算ノードを制御する ECP Agent ソフトウェアと ECP Manager クラスター間でコマンド処理および制御処理を行うために、軽量のパブリッシュ / サブスクライブ・メッセージング・バスを提供します。この拡張性のあるメッセージバスは、Extensible Messaging and Presence Protocol (XMPP) に基づいています。XMPP は、軽量のミドルウェアとしての役割に適したリアルタイム通信のためのオープン・テクノロジーです。XMPP は、ほとんどのファイアウォール間での接続が可能な、標準の HTTP (tcp/80) ポートと HTTPS (tcp/443) ポートで動作します。

テストベッドでの実装では、IaaS 機能を提供するために必要な Enomaly ECP SPE のすべての機能 (プロビジョニング、監視、仮想マシン管理、高可用性など) をサポートしています。以下の項では、ソフトウェア実装、ハードウェア・テストベッド、実行されたテストケース、およびクラウド設計時の考慮事項について詳しく説明します。

テストベッドの計画の概要

ハードウェアの説明

クラウドのハードウェア・インフラストラクチャーでは、顧客がクラウドベースのサービスをホストするために、さまざまなハードウェア・コンポーネントが必要となります。標準的なハードウェア・コンポーネントとしては、計算負荷をホストするサーバー・プラットフォーム、データをホストするストレージ・プラットフォーム、内部および外部トラフィックを管理するネットワーク・コンポーネント、その他のデータセンター・インフラストラクチャー・コンポーネントなどがあります。

テストベッドでは、インテル® Xeon® プロセッサ 5500 番台を使用しました [4] [5]。これにより、消費電力とスペースを削減し、運用コストを大幅に削減しながら、パフォーマンスを向上させる新しいクラウド・データセンターを設計するための基盤が提供されます。図 3 は、テストベッドの物理アーキテクチャーを示しています。

インテル® Xeon® プロセッサ 5500 番台は、クラウドのサーバー・パフォーマンスを最大限に高めるうえで役立つ機能を備えています [6]。次のような機能があります。

- インテリジェントなパフォーマンス：ビジネス要件とアプリケーションのパフォーマンスの要件に合わせて、プロセッサの動作周波数を自動的に変更します。
- 自律的な省電力機能：ワークロードに応じて消費電力を調整することで、消費電力当たり性能を最適化し、運用コストを削減します。
- 柔軟な仮想化環境：仮想化環境でのクラス最高水準のパフォーマンスと管理性を提供し、インフラストラクチャーの強化とコスト削減を実現します。

物理アーキテクチャー

インテル / Enomaly テストベッドの要件を満たすために、以下の仕様に従い、「Enomaly ECP SPE の基本的な導入アーキテクチャー」(4 ページの図 1) に基づく小規模な実装を導入しました。

システム設計

クラウド設計の基本理念に従って、クラウド設計を 4 つの機能ブロック (クラウドベースのサービスをホストするために必要なクラウド、ストレージ、ネットワーク、コンピューティングの各要素を管理するためのインフラストラクチャー制御) に分けました。各種機能ブロックを処理するために、サーバーをどのように分散したかについては、表 1 に詳しく示しています。

さらに、分離、セキュリティ、QoS の各要件を満たすために、ネットワークを次のように分割しました。

- セルフサービス・ポータル経由でクラウドにアクセスするエンド顧客用の外部顧客ネットワーク
- すべてのコマンド機能と制御機能を管理する際に使用する社内管理ネットワーク
- 計算ノードでホストされる仮想マシンのデータを管理するための社内プライベート・ネットワーク

ストレージ・ネットワークには、2 つの Cisco* 3750G (1G) スイッチと、Extreme Networks* Summit* X650-24t (10G) を 1 つ使用しました。すべてのスイッチは、合計 3 つのサブネットで「すぐに使用できる」状態 (1 つのサブネットに構成された全 48 ポートで VPN 構成不要) にあります。

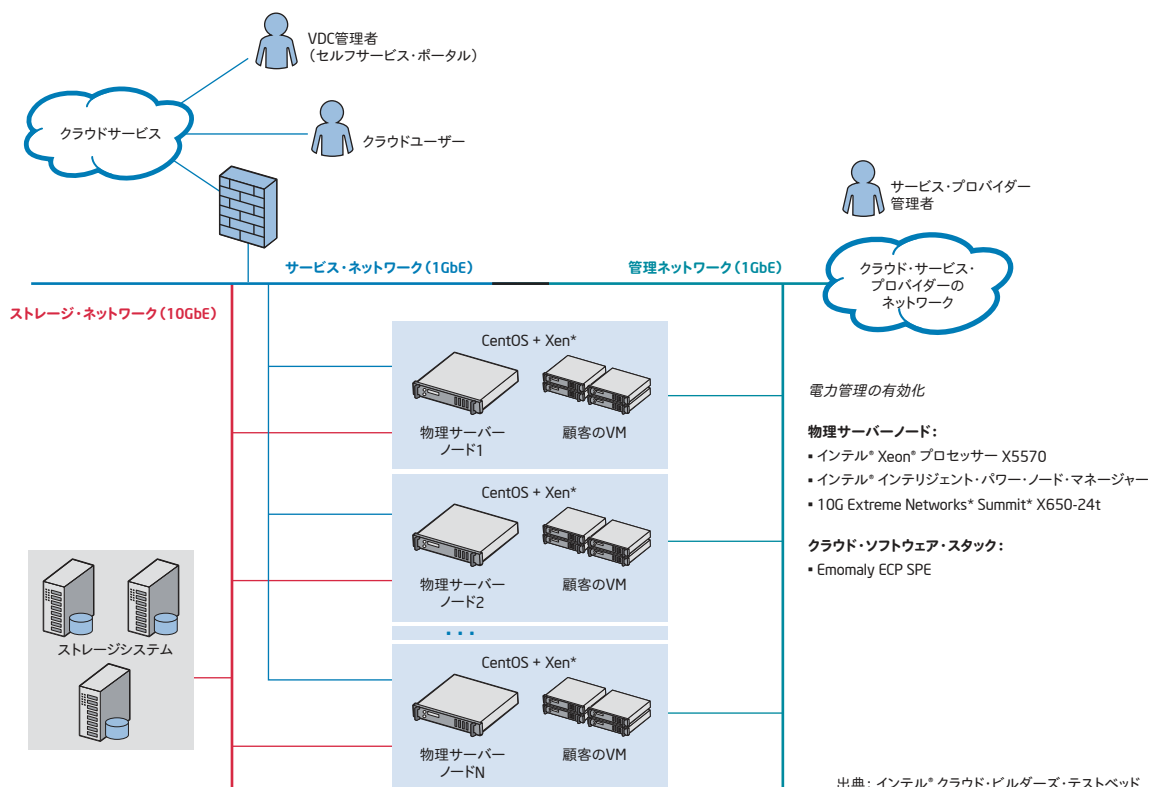


図 3. テストされた物理アーキテクチャー

表 1. クラウド・テストベッドのシステム構成

システム	プロセッサ構成	その他の情報
ECP マスターノード× 1 および ECP エージェント・ノード× 4	インテル® Xeon® プロセッサ X5570 ^Δ	<ul style="list-style-type: none"> フォームファクター: 1U ラックマウント型サーバー プロセッサ: インテル® Xeon® プロセッサ 5500 番台 (クアッドコア、動作周波数: 2.93GHz)x2 メモリー: 32GB ストレージ: 4 × 500GB HDD SATA2 サービス・ネットワークと管理ネットワーク: インテル® 82576 ギガビット・ネットワーク接続 ストレージ・ネットワーク: インテル® 82598EB 10 ギガビット AT2 サーバーアダプター
ストレージサーバー× 1	インテル® Xeon® プロセッサ E5345 ^Δ	<ul style="list-style-type: none"> フォームファクター: 2U タワー型サーバー プロセッサ: インテル® Xeon® プロセッサ 5300 番台 (クアッドコア、動作周波数: 2.33GHz)x2 メモリー: 16GB ローカルストレージ: 1 × 160GB HDD SATA 拡張ストレージ: 10 × 160GB SDD
プロキシサーバー× 1	インテル® Xeon® プロセッサ	<ul style="list-style-type: none"> フォームファクター: 1U ラックマウント型サーバー プロセッサ: インテル® Xeon® プロセッサ (シングルコア、動作周波数: 2.80GHz)x2 メモリー: 2GB RAM ストレージ: 2 × 160GB HDD SATA
ネットワーク	Summit® X650-24t	<ul style="list-style-type: none"> ポート: 24 × 10GBASE-T ポート (ポート 1 ~ 24)、4 × 1000BASE-X (SFP) ポート (ポート 25 ~ 28)、2 × SummitStack ポート (残り 2 つの 10GBASE-T ポートと共有 / 専用、10Gbps、自動ネゴシエーションなし) VLAN: 802.1Q、ポートベース VLAN とタグベース VLAN

表 2. ネットワーク IP 構成

	ホスト名	ストレージ・ネットワーク	プライベート・ネットワーク	サービス・ネットワーク
ストレージサーバー	ECPstorage	192.168.182.240	192.168.181.240	172.18.1.112
ECP マスターノード	ECP-master	192.168.182.100	192.168.181.100	172.18.1.105
ECP ノード 01	ECP01	192.168.182.101	192.168.181.101	172.18.1.106
ECP ノード 02	ECP02	192.168.182.102	192.168.181.102	172.18.1.107
ECP ノード 03	ECP03	192.168.182.103	192.168.181.103	172.18.1.108
ECP ノード 04	ECP04	192.168.182.104	192.168.1821.104	172.18.1.109

本リファレンス・デザインでは、サーバーおよびストレージのホスティングに参加するノード (ECP-master、ECP01、ECP02、ECP03、ECP04、および ECPstorage) の静的 IP アドレスを予約しました。

追加のサーバーをキャッシュ・プロキシ・サーバーとして機能するよう構成しました。この作業は、サーバーの起動および稼働時に使用するプロセスを高速化することを目的に行いました。各サーバーは、Enomaly ECP SPE のクリーンコピーを使用してインストールされているため、インターネットから更新プログラムとパッケージを入手する必要があります。キャッシュ・プロキシ・サーバーは、これらのパッケージをキャッシュしてプロセスを高速化するように構成されています。

技術レビュー

インストールの概要

この項では、インテル / Enomaly クラウド・インフラストラクチャーのインストール・プロセスについて説明します。クラウド・インフラストラクチャーを構築するために、ハードウェア、ソフトウェア、メモリー、ネットワーク、ストレージの各リソースが十分にあること、およびネットワーク全体の DHCP 接続を検証しました。次に、ストレージ要素、スイッチ、および VLAN の設定を構成し、ECP マスターノードと 4 つのエージェント・ノードをインストールして、ネットワークおよびデータベース接続を確認しました。新しく構成した ECP 環境をテストするために、VM を作成し、VM のプロビジョニングと管理を検証しました。特定のデバイスおよびサーバーの構成パラメーターを含めた各手順の詳細については、Enomaly ECP SPE / インテル・テストベッドのインストールの詳細に関するドキュメントを参照してください [7]。

ユースケースの詳細

アクター

- サービス・プロバイダー (SP)
- サービス利用者 (SC1, SC2)

ユースケースの概要

クラウド・テストベッド App Center は、CentOS 5.4 (64ビット) のインスタンスを使用してプロビジョニングされました。クラウド実装のテストフェーズでは、以下の 14 個のユースケースが正常に実行されました。

前提条件:

- クラウド管理ソフトウェアとして、Enomaly ECP SCE ソフトウェアがインストールされ、使用準備ができていないこと。
- 計算ノードとストレージノードがインストールされ、登録されていること。
- SC1 および SC2 のアプリケーション・サービス (Service 1 と Service 2) が VM にパッケージングされ、計算ノードに導入されていること。

ユースケース:

- アプリケーションの仮想マシンのパッケージング: アプリケーション・サービス・パッケージを導入する。
- ユーザーの作成: 管理者が管理者ポータルから 2 人のユーザー (SC1, SC2) を作成できることを確認する。
- SC1, SC2 : Service 1, Service 2 のインスタンスの作成: IP アドレスやストレージへのリンクを含む、Service 1 と Service 2 を構成する VM をインスタンス化する。
- SC1, SC2 : Service 1, Service 2 の状態の監視: 新しく作成した VM の状態を観察する。
- VM の複製: 2 人のユーザー (SC1, SC2) が VM を複製できることを確認する。
- SC1 : Service 1, Service 2 のスケールアウト: app フロントエンド VM を追加し、負荷分散プールに追加する。アプリケーションの拡張性をテストする。
- ネットワークの分離: VM 間でのネットワークの分離を確認する。
- SC1 : app フロントエンド VM の終了: 負荷分散プールから VM を削除して終了し、結果を観察する。
- VM の構成管理: SC1 および SC2 に属する VM にログインして、VM の構成を確認する。
- 課金レポートの生成: クラウドの利用者 (SC1, SC2) が課金レコードを調べることができることを確認する。

- SP : 既存のクラスターへのベアメタル・キャパシティの追加: 既存のクラスターに新しい物理サーバーを追加する。
- SC1, SC2 : Service 1, Service 2 のスケールアウト: Service 1 と Service 2 の両方で、業種別アプリケーションの拡張性をテストする。
- SP : サーバーの障害: クラスターが引き続き稼働していることを確認する。
- SC1, SC2 : Service 1, Service 2 のシャットダウン: アプリケーション・サービスと、ユーザー SC1 および SC2 へのリモートアクセスを終了する。

実行と結果

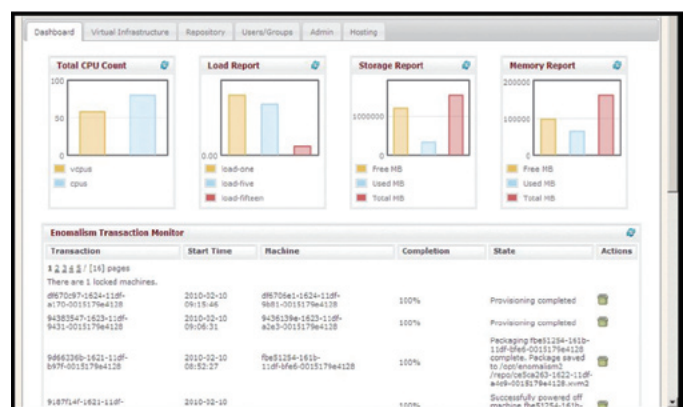
前述のテストケースは、すべて正常に実行されました。以下の項では、各手順のスクリーンショットを含め、各テストケースの入力とシステムの応答について詳しく説明します。特に指定のない限り、ユースケースはすべて、セルフサービス Web UI ポータルから実行されています。

セットアップとソフトウェアの検証

- Web UI ポータル (設定: <http://172.18.1.105:8080>) から "admin" として正常にログインします。



- ダッシュボードを監視して、クラスターが稼働していることを確認します。ダッシュボードには、クラスターの負荷および実行中のトランザクションの集計とともに、CPU 使用量が示されます。



- "App Center" のホームページにアクセスし、ECP SPE 3.0.4 に用意されている "centos54" VM テンプレートを使用して VM をインストールします。テストでは、VM 名として "test"、ハードウェア・テンプレートとして "Medium" を使用し、その他のオプションにはデフォルト設定を使用しました。VM のインストールの進行状況は、[Home] ページで監視できます。

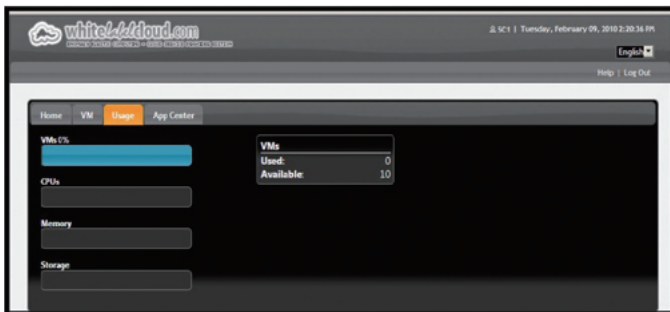
Small:i686 CPU Arch 1024 Memory	xen-hvm Hypervisor 1 CPUs
Medium:i686 CPU Arch 2048 Memory	xen-hvm Hypervisor 2 CPUs
Large:x86_64 CPU Arch 8192 Memory	xen-hvm Hypervisor 8 CPUs

3. **[Hosting/NETWORK]** ページに移動し、4 つの VLAN を作成します。

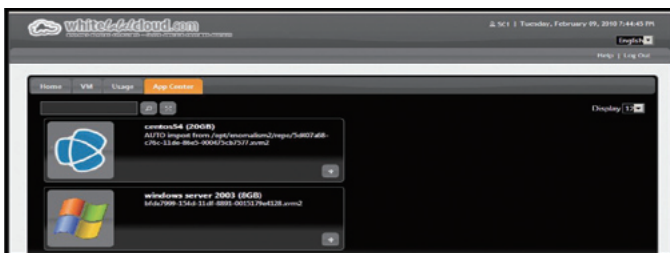
```
VLAN100:100 VLAN ID
VLAN200:200 VLAN ID
VLAN300:300 VLAN ID
VLAN400:400 VLAN ID
```

4. **[Users/Groups]** — **[EDIT PERMISSIONS]** ページに移動し、グループ G1 と G2 に「読み取り」権限を付与します。

5. ログアウトして「SC1」としてログインし、**[Usage]** ページで現在のリソース使用量と割り当てを確認します。



6. 同じユーザー（SC1）で、**[App Center]** ページに移動して、承認済みテンプレートを確認します。



7. ログアウトし、ユーザー SC2 で上記の 2 つの手順を繰り返して、割り当てと VM 設定を確認します。

複数のユーザーによるサービス・インスタンスの作成

1. **[App Center]** ページに移動し、ECP SPE 3.0.4 に用意されている「centos54」VM テンプレートを 사용하여 VM をインストールします。ハードウェア・テンプレートとして「small」、VM 名として「centos54-1」を使用します。**[VM]** ページにアクセスして、「centos54-1」が正常に作成されているかどうかを確認します。**[Usage]** ページに移動すると、リソース使用量と割り当てが更新されているかどうかを確認できます。

2. 1 分ほど待ってから、VM 「centos54-1」の **[Details]** ページを開きます。**[Network]** タブに移動し、VM の IP アドレスが正常にプロビジョニングされているかどうかを確認します。



3. VM 「centos54-1」への VNC 接続を開き、アカウント情報を使用して VM にログインします。

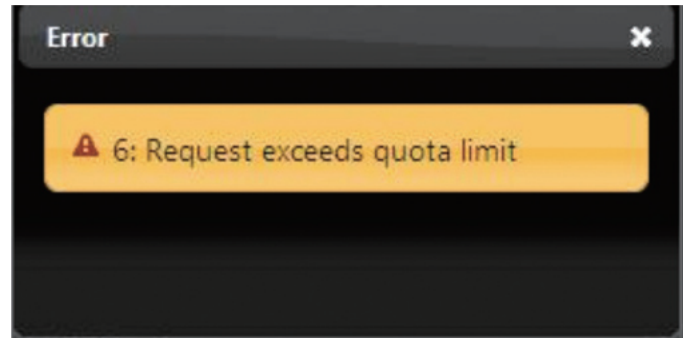
```
$ ping www.intel.com
この ping は成功します。
```

サービスの監視

1. 下記のように追加の VM をインストールし、各 VM が正常に作成されていることを確認します。

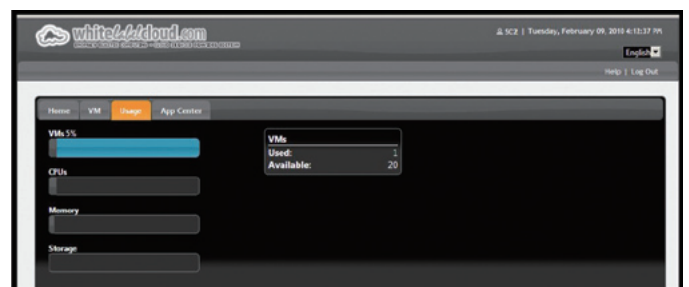
```
VM名: "centos54-2" / ハードウェア・テンプレート: "Medium"
VM名: "centos54-3" / ハードウェア・テンプレート: "Large"
VM名: "centos54-4" / ハードウェア・テンプレート: "Large"
```

2. **[App Center]** ページで、「centos54」VM テンプレート（VM 名: 「exceed」、ハードウェア・テンプレート: 「Large」）を使用して、VM をもう 1 つインストールします。ただし、割り当て制限を超えるため、今回は失敗の通知が表示されます。



3. 「admin」としてログアウトし、ユーザー「SC2」としてログインします。

4. **[App Center]** ページに移動し、「windows server 2003」VM テンプレート（VM 名: 「win2003-1」、ハードウェア・テンプレート: 「Small」）を使用して VM をインストールし、VM が正常に作成されていることを確認します。



- VM "win2003-1" への VNC 接続を開き、アカウント情報を指定して VM にログインします。

```
a. $ ping www.intel.com
b. この ping は成功します。
```

- 上記の手順を繰り返して、以下の VM をインストールします。

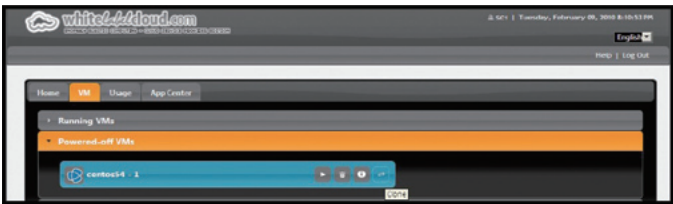
```
VM名: "win2003-2" / ハードウェア・テンプレート: "Medium"
VM名: "win2003-3" / ハードウェア・テンプレート: "Large"
VM名: "win2003-4" / ハードウェア・テンプレート: "Large"
VM名: "win2003-5" / ハードウェア・テンプレート: "Large"
VM名: "win2003-6" / ハードウェア・テンプレート: "Large"
```

- ログアウトして "admin" としてログインし、ダッシュボードで更新されたリソースレポートを確認します。

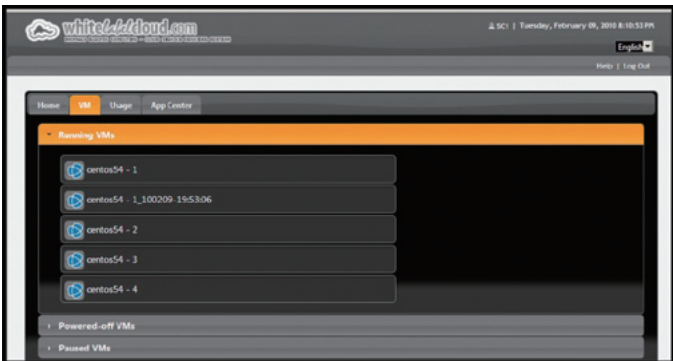


複数のユーザーによる VM の複製

- [VM] ページに移動し、VM "centos54-1" の電源をオフにします。VM が [Powered-off VMs] グループに移動したら、この VM を選択して複製します。複製した VM は電源が自動的にオンになります。複製した VM には、元の VM 名の末尾に現在の日付と時刻が付加された名前が付けられます。



- 複製が正常に完了し、"centos54-1" および複製されたコンポーネントの電源がオンになると、複製された VM が [VM] ページに反映されます。



ネットワークの分離

- ユーザー "SC1" としてログインし、すべての VM の電源をオフにします。VM "centos54-1" のネットワーク設定を再構成します。**[Network]** タブにアクセスします。ネットワークを **[default]** から **[VLAN100]** に再構成します。"centos54-2" に対して同じ手順を繰り返します。**[Network]** タブにアクセスします。ネットワークを **[default]** から **[VLAN200]** に再構成します。

- VM "centos54-1"、"centos54-2"、および "centos54-1" の複製した VM の電源をオンにします。VM "centos54-1" および "centos54-2" はともに分離されているので、DHCP サーバーから引き続き IP を取得できるのは、"centos54-1" の複製した VM だけであることを確認します。

- VM "centos54-1" への VNC 接続を開き、VM にログインします。次のコマンドを使用して、ネットワークの IP アドレスを再構成します。

```
# ifconfig eth0 192.168.190.101 netmask 255.255.255.0
```

- VM "centos54-2" への VNC 接続を開き、VM にログインします。次のコマンドを使用して、ネットワークの IP アドレスを再構成します。

```
# ifconfig eth0 192.168.190.102 netmask 255.255.255.0
```

- ログアウトして "SC2" としてログインし、すべての VM の電源をオフにします。VM "win2003-1" の **[Details]** ページを開き、**[Network]** タブに移動します。ネットワークを **[default]** から **[VLAN100]** に再構成し、VM "win2003-3" のネットワークを **[default]** から **[VLAN300]** に再構成します。

- VM "win2003-1"、"win2003-3"、および "win2003-1" の複製した VM の電源をオンにします。VM "win2003-1" および "win2003-3" はともに分離されているので、DHCP サーバーから引き続き IP を取得できるのは、"win2003-1" の複製した VM だけであることを確認します。

- VM "win2003-1" と "win2003-3" への VNC 接続を開き、VM にログインします。ネットワークの IP アドレスを一意的アドレスに再構成します。

- ログアウトして、ユーザー "SC1" としてログインします。VM への VNC 接続を開き、VM にログインします。次のように、他の VM に対して ping を実行します。

```
$ ping centos54-2 // この VM は同じ VLAN に存在しないので応答なし
$ ping win2003-1 // この VM は同じ VLAN に存在するので応答あり
$ ping win2003-3 // この VM は同じ VLAN に存在しないので応答なし
```

VM の構成管理

1. [Virtual Infrastructure/INFRASTRUCTURE] ページに移動し、[SC2/ECP01] の下の VM “SC2_win2003-2” のページを開きます。VM の CPU、メモリー、HD の構成が [default] から [VLAN200] に変更されていることを確認します。



複数のユーザーの課金

1. 課金データは、プログラムからアクセスできるように提供されていますが、対象となる開始日 / 開始時刻と終了日 / 終了時刻を含む特殊な URL を指定すると、課金データを手動で取得できます。例えば、2010年2月9日午前 11:00.00 から 2010年2月11日午前 11:00.00 までの課金情報を取得するには、http://172.18.1.105:8080/modules/billingreports/?start_date=2010:02:09:11:00:00&end_date=2010:02:11:11:00:00 にアクセスします。

user	user_uuid	Small	Medium	Large	Total MBytes
admin	7eabba12-12fe-11dd-8fd0-0019d2b28af0	0	0	0	0
customer	b0e229cc-115f-11df-83ba-0015179e4128	5	31	8	9729
SC1	25576b1c-1524-11df-9d72-0015179e4128	88	49	88	358400
SC2	52db6d35-1524-11df-ab85-0015179e4128	133	44	175	81920

2. この出力を “billing.csv” という名前で保存します。

新しいサーバーの追加

1. [Virtual Infrastructure/INFRASTRUCTURE] ページにアクセスし、既存の ECP ノードを確認します。4つの ECP ノード (ECP-master, ECP01, ECP02、および ECP03) が表示されます。



2. ECP04 にログインし、エージェント・ノードをインストールするために ECP SPE 3.0.4 のインストールを開始します。詳細については、Enomaly ECP SPE/ インテル・テストベッドのインストールの詳細に関するドキュメントを参照してください [7]。Web UI ポータルで、[Virtual Infrastructure/INFRASTRUCTURE] ページにアクセスします。ECP04 が既存の ECP ノードに追加されています。

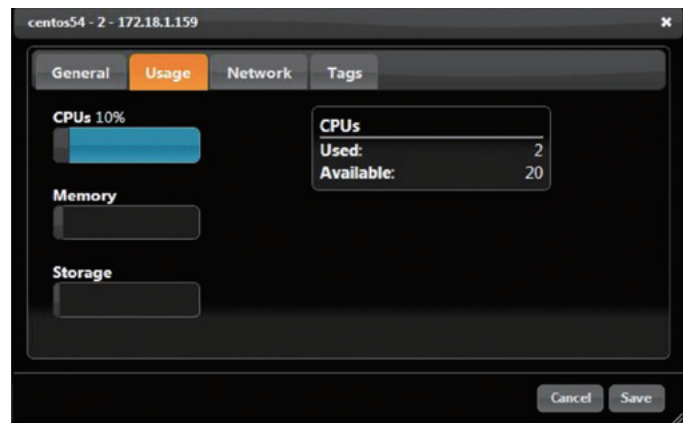
サービスのスケールアップとスケールダウン

1. Web UI ポータル (<http://172.18.1.105:8080>) から “SC1” としてログインします。[VM] ページにアクセスし、VM “centos 54-2” の電源をオンにします。この VM の [Details] ページを開き、[Usage] タブに移動して、この VM の現在の CPU、メモリー、HD の構成を確認します。
2. VM “centos54-2” の電源をオフにし、[Details] ページを開いて、ハードウェア・テンプレートを [Medium] から [Large] に変更します。

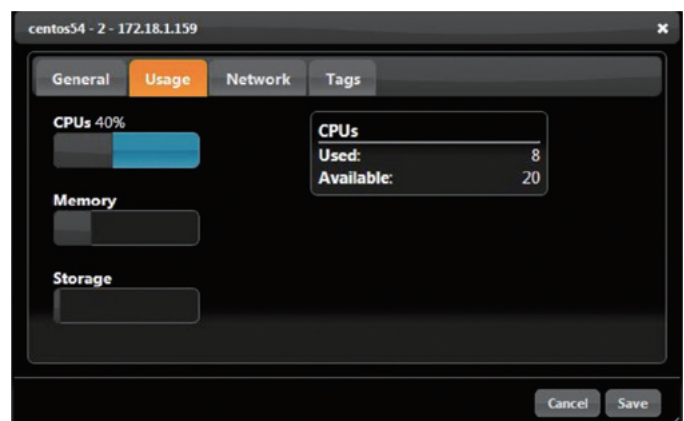
```
Small:i686 CPU Arch      xen-hvm Hypervisor
1024 Memory    1 CPUs

Medium:i686 CPU Arch    xen-hvm Hypervisor
2048 Memory    2 CPUs

Large:x86_64 CPU Arch   xen-hvm Hypervisor
8192 Memory    8 CPUs
```



3. VM “centos54-2” の電源をオンにし、[Details] ページを開きます。[Usage] タブに移動して、この VM の現在の CPU、メモリー、HD 構成を確認します。



```
# cat/proc/cpuinfo > cpuinfo.info
```

(cpuinfo.infoからの部分出力)

```
processor:0
vendor_id:GenuineIntel
model name: Intel® Xeon® CPU X5570 @ 2.93GHz
processor:1
vendor_id:GenuineIntel
model name: Intel® Xeon® CPU X5570 @ 2.93GHz
processor:2
vendor_id:GenuineIntel
model name: Intel® Xeon® CPU X5570 @ 2.93GHz
processor:3
vendor_id:GenuineIntel
model name: Intel® Xeon® CPU X5570 @ 2.93GHz
```

```
# cat/proc/meminfo > meminfo.info
```

(meminfo.infoからの部分出力)

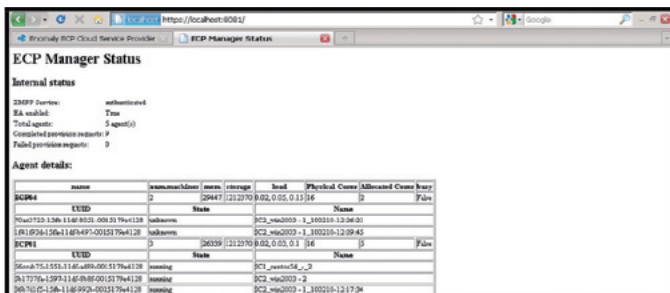
```
MemTotal:3893932 kB
MemFree:3813588 kB
```

障害シナリオ

1. 次のコマンドを使用して、ECP-master ノードへの SSH トンネルを開きます。

```
# ssh-L 8081:127.0.0.1:8081 root@172.18.1.105
```

2. ECP Manager Status レポート (<https://localhost:8081>) に接続し、既存の ECP ノードを確認します。すべてのノードがアクティブになっています。
3. ECP04 を再起動します。ECP04 に取り消し線が付けられ、ECP04 で実行されている VM の状態が約 10 秒で実行中から不明に変更されます。



4. ECP04 が約 5 分で稼動状態に戻ると、ECP04 の取り消し線が削除されます。ECP04 で実行されているすべて VM が ECP01 に移動し、実行状態に変更されています。

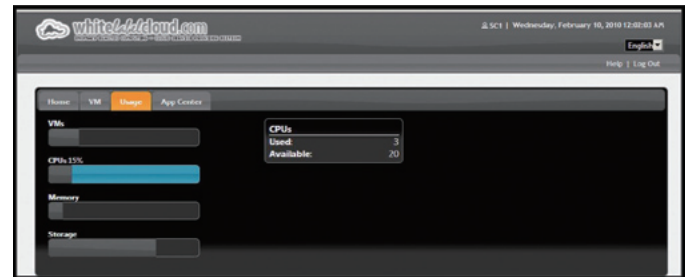


5. ECP-master を再起動して次の点を観察します。

- ECP-master が稼動状態に戻るまで、Web UI ポータルと ECP Manager Status レポートは利用できません。
- ECP エージェント・ノードは引き続き稼動しています。ノードで実行されている VM に ping を実行して確認します。

サービスのシャットダウン

1. Web UI ポータル (<http://172.18.1.105:8080>) から "SC1" としてログインします。
2. "centos54-1" (Small) と "centos54-2" (Medium) を除くすべての VM の電源をオフにします。スナップショットに、CPU 割り当ての 15% しか現在使用されていないことが示されます。



3. VM "centos54-1" (Small) と "centos54-2" (Medium) の電源をオフにします。
4. [Usage] ページに移動し、リソース使用量と割り当てを確認します。CPU 割り当てが 0% に下がります。

観察と分析

Enomaly ECP SPE は、サービス・プロバイダー (収益を生み出す顧客向けのビジネスユニット、または企業内の IT サービス組織) が、セルフサービスのオンデマンド・インフラストラクチャー・ソリューションを顧客またはユーザーに提供できるようにするためのソリューションです。前述のテストケースでは、このためにプラットフォームの中心的な機能を検証しました。

環境のストレステスト

障害モードの検証

Enomaly ECP SPE の HA モジュールの使用時には、さまざまな障害モードで VM とホストが自動復旧されます。稼動本番環境に移行する前に、すべてのホスティング環境のストレステストを徹底的に行う必要があります。少なくとも、以下のシナリオをテストすることをお勧めします。

A. ホストマシンの再起動 (ホストの喪失は < 10 分) :

1. Manager Status レポート (<https://<プライマリー・ホスト名>:8081>) を調べます。
2. ホストマシンの名前に取り消し線が付けられ、VM が不明状態に移行していることがわかります。
3. ホストが復帰すると、エージェントが名前を取り消し線を削除し、VM が「オフ」状態になります。
4. しばらくすると、すべての VM が再起動することを観察します。

B. ホストマシンの電源障害 (ホストの喪失 > 10 分) :

1. Manager Status レポート (<https://<プライマリー・ホスト名>:8081>) を調べます。
2. 10 分経つと、ホストマシンの名前に取り消し線が付けられ、VM が不明状態に移行することがわかります。
3. すべての VM が他のホストに移動し、「実行中」状態になります。
4. ホストが復帰すると、取り消し線が削除されます。エージェントは実行中の VM がないことを示しますが、プロビジョニング・ジョブをいつでも実行できる状態になります。

C. ホストの断続的なネットワーク喪失 (ネットワークの喪失 < 10 分) :

1. Manager Status レポート (<https://<プライマリー・ホスト名>:8081>) を調べます。
2. 障害は検出されていないので、エージェントは取り消し線を付けません。
3. ネットワークの回復後、すべての VM が再稼動し始めるまで、VM はこのホストからの ping に応答できません。

D. ホストの永続的なネットワーク喪失 (ネットワークの喪失 > 10 分) :

1. Manager Status レポート (<https://<プライマリー・ホスト名>:8081>) を調べます。
2. 10 分経つと、ホストマシンの名前に取り消し線が付けられ、VM が不明状態に移行することがわかります。
3. すべての VM が他のホストに移動し、「実行中」状態になります。
4. ネットワークが復帰すると、取り消し線が削除されます。エージェントは実行中の VM がないことを示しますが、プロビジョニング・ジョブをいつでも実行できる状態になります。

E. プライマリー・ホストの喪失:

1. この状態では Web UI は応答しなくなりますが、すべてのホストで VM が引き続き実行されることを観察します。
2. プライマリー・ホストがサービスに復帰すると、すべてのコマンドと制御が管理者とユーザーに戻ります。

パフォーマンスの検証

ECP クラスタでテストする主なパフォーマンス要件は、VM で使用可能なディスク I/O です。これをテストするには、次の手順を実行します。

1. 各ホストに Bonnie++ をインストールし、NFS 共有へのディスク I/O をテストします。/var/lib/xen 共有ディレクトリーから、パフォーマンスのベースライン値を入手する必要があります。いずれかのホストが大きく異なる値を示している場合は、NFS のチューニングが必要と考えられます。このテストは、同時に実行するのではなく、順次実行する必要があります。
2. VM 内で Bonnie++ をインストールします。返された値がホストマシン自体の値の 60 ~ 80% 以内であるかどうかを確認します。オーバーヘッド損失が予想されますが、60% 未満の場合は構成の問題を示していると考えられます。

Bonnie++ は、ハードディスク・ドライブとファイルシステムのパフォーマンスに関する簡易テストを多数実行することを目的とした、オープンソースのベンチマーク・スイートです。このベンチマークは、<http://www.coker.com.au/bonnie++/> (英語) からダウンロードできます。

次のステップ

前のリファレンス・デザインでは、マルチテナント・クラウドを実装しています。ただし、この設計では、各ノードのソフトウェアと BIOS が、実際に承認されたバージョンに間違いがないことを確認するための手段が限られています。インテル® Xeon® プロセッサ 5600 番台では、信頼性のあるマルチテナンシー支援技術を採用しており、クラウド内のリソースプールに参加することをサーバーに許可する前に、BIOS とハイパーバイザーの主要コンポーネントの改ざんの有無を確認できます。次世代のインテル® Xeon® プロセッサ 5600 番台は、次のような機能を備えています。

1. **インテル® トラストド・エグゼキューション・テクノロジー (インテル® TXT) [8]** : インテル® TXT は、プロセッサ、チップセット、BIOS、および Trusted Platform Module (TPM) の機能を使用して、BIOS やオプションの ROM からハイパーバイザーやオペレーティング・システムに至るまで、プラットフォーム・コンポーネントの堅牢な検証基盤を実現し、根元から「継承された信頼」を実現するためのメカニズムを提供します。インテル® TXT では、継承された信頼 (信頼のルート) は、プラットフォームにおいて最も保護されたコンポーネントと考えられるプロセッサ本体から始まります。
2. **インテル® Advanced Encryption Standard - New Instructions (インテル® AES-NI) [8]** : インテル® AES-NI は、インテル® Xeon® プロセッサ 5600 番台で提供される新しい命令セットです。これらの命令により、FIPS Publication 197 で定義された Advanced Encryption Standard (AES) を使用した、データのセキュアな暗号化と復号を高速化できます。現在、AES は最も有力なブロック暗号化であり、各種プロトコルで使用されているため、この新しい命令はさまざまなアプリケーションで役立ちます。
3. **ECP High Assurance Edition** : High Assurance Edition は、Enomaly ECP Service Provider Edition の機能セットを拡張し、独自の高度なセキュリティー機能セットを備えています。この機能セットは、市場で入手できるクラウド・コンピューティング・サー

ビス製品で提供されるセキュリティよりも、さらに高レベルのセキュリティを必要とする顧客のニーズを満たすのに適しています。Enomaly は、ハードウェア・アシストによる独自のメカニズムによってセキュリティを継続的に保証することで、信頼できるクラウド・プラットフォームを提供します。例えば、顧客に対して次の内容を保証できます。

- ハードウェアが変更され、顧客の知らないストレージメディアにデータが複製されていないこと
- ハイパーバイザーが変更され、メモリの状態や VM イメージがコピーされていないこと
- 悪意のある kernel モジュールがゲスト OS に挿入されていないこと

4. 電力管理：消費電力を最適化するポリシーとともに、インテル® インテリジェント・パワー・ノード・マネージャーおよびインテル® データ・センター・マネージャー [9] を利用します。ユースケースを実装すると、消費電力制限によってサーキットブレーカーの遮断やデータセンターのホットスポットを回避できます。インテル® インテリジェント・パワー・ノード・マネージャーを利用した Baidu の事例については、[10] を参照してください。

考慮事項

拡張性

クラウド・ソリューションの拡張性は、次の要素によって影響を受ける可能性があります。

- ネットワークのテクノロジー (10GigE など) とアーキテクチャー
- 選択したストレージ・アーキテクチャー
- 計算ノードと管理ノード用のサーバー・ハードウェアの選択

考慮すべきもう 1 つの興味深い選択肢としては、ハードディスクの代替としてソリッドステート・ドライブ (SSD) を使用することが挙げられます。SSD によって、クラウドのパフォーマンスが大幅に向上する可能性があります。また、クラウド実装を計画するときには、セキュリティを第一に考える必要があります。以下に、これらの各トピックについて簡単に説明します。

ネットワーク・テクノロジー・アーキテクチャー

Enomaly ECP SPE は、複数のネットワーク・テクノロジー・アーキテクチャーをサポートしています。このテストベッドでは、非常に単純なネットワーク・トポロジーを選択しました。今回のテストケースでこのテストベッドを機能させるためには十分な選択でしたが、稼働本番環境に展開する場合は、より高度なテクノロジーとアーキテクチャー (10-GigE、チャンネル・ボンディング・テクノロジー、高度にセグメント化されたネットワーク・アーキテクチャーなど) が適していると考えられます。

ストレージ・アーキテクチャー

Enomaly ECP SPE は、複数のストレージ・アーキテクチャーをサポートしています。このテストベッドでは、最も簡単な選択肢である単一の NFS を採用しました。今回のテストケースでは特に問題なく機能しましたが、稼働本番環境に展開する場合は、より高度なアーキテクチャーを選択することをお勧めします。

ハードウェアに関する考慮事項

プロセッサとサーバー全体のパフォーマンスに関して考慮すべき項目についての詳しい説明は、このガイドの対象範囲外となります。ただし、プロセッサのアーキテクチャーや、ダイレクト I/O 向けインテル® パーチャライゼーション・テクノロジーのようなプロセッサで提供される特定の機能セットなどの要素が、クラウド・プラットフォームで実行される仮想マシンのパフォーマンスに大きな影響を与えることに注意してください。インテル® Xeon® プロセッサ 5500 番台やインテル® Xeon® プロセッサ 5600 番台など、仮想化を I/O やネットワークまで包括的にサポートする機能セットを備えた高性能のサーバー・プロセッサを使用することを強くお勧めします。インテル® パーチャライゼーション・テクノロジーの詳細については、[11] を参照してください。

ソリッドステート・ドライブ (SSD)

SSD を使用すると、ストレージノード (およびローカルストレージを使用する場合は計算ノード) のパフォーマンスと、クラウドの全体的な電力消費量に良い影響を与えることがあります。この点については、この事例では具体的なテストは行われませんでした。

セキュリティに関する考慮事項

セキュリティは、IaaS の選択および管理における重要な考慮事項です。サービス・プロバイダーとエンドユーザー組織の両方の観点による、クラウドのセキュリティのベスト・プラクティスに関する詳しい説明は、このドキュメントの対象範囲外となります。ただし、次の点を考慮してください。

- 従来の物理ホスト環境でホストのセキュリティのために確立されたベスト・プラクティス (パスワード管理、パッチ管理、サーバーの強化、アンチマルウェアなど) は、IaaS プラットフォームで仮想ホストを運用する場合にも同様に適用する必要があります。
- Enomaly ECP などの IaaS プラットフォームでは、ハードウェア・アシストによる完全な仮想化を使用して、各仮想サーバーを完全に分離します。そのため、仮想サーバーは、それぞれ独自の仮想ハードウェアや専用のオペレーティング・システム・インスタンスなどを使用できます。これに対して、「ドメイン」または「コンテナ」に基づくクラウド・プラットフォームの場合、一部の仮想ハードウェアとオペレーティング・システム・コンポーネントが仮想ホスト間で共有されるため、新たな攻撃手段が生み出されます。
- Enomaly ECP では、各顧客のネットワーク・トラフィックを 1 つ以上のプライベート VLAN に分離することによって、さまざまな顧客に属する仮想ホストをネットワーク・レベルでさらに分離できます。

Enomaly ECP High Assurance Edition では、インテル® Xeon® プロセッサ 5600 番台のインテル® トラストド・エグゼキューション・テクノロジー (インテル® TXT) 機能を利用して、ハッキング、改ざん、および管理上の不正な変更から強力に保護された IaaS 環境を実現します。

さらに、Enomaly は、最も高度なセキュリティ要件を満たすために、Enomaly ECP プラットフォームの High Assurance Edition (HAE) も提供しています。

追加情報

インテル® クラウド・ビルダーズ：<http://intel.com/software/cloudbuilder/> (英語)

インテル® Xeon® プロセッサ：http://www.intel.com/p/ja_JP/products/server/processor/

Enomaly：<http://www.enomaly.com/> (英語)

用語集

使用する用語についてあいまいにならないように、このガイドで使用されている概念の一部について、その定義を以下に示します。

クラウド・コンピューティング：IT の利用と提供の進化形態。クラウド・コンピューティングでは、柔軟性のある従量課金ビジネスモデルを使用し、インターネットを介してセルフサービス・ベースで IT を利用および提供できます。

ドメイン：ハイパーバイザーで提供される仮想化マシン上で実行されている、オペレーティング・システム(コンテナ仮想化の場合はサブシステム)のインスタンス。

Enomaly Elastic Computing Platform* (ECP)：サービス・プロバイダーまたは企業のクラウド・コンピューティング・プラットフォームを構成するソフトウェア製品。

HA：高可用性。

ハイパーバイザー：一連の仮想マシンでノードの仮想化を可能にするソフトウェアのレイヤー。ノード自体と構成が異なる可能性のある 1 つ以上の仮想マシンをサポートします。

LVM：論理ボリューム・マネージャー。

ノードまたはホスト：単一の物理マシン。

プール：ひとまとまりのストレージ領域を取得し、複数のボリュームに分割するための方法。プールを使用して、物理ディスク、NFS、iSCSI ターゲット、ホストアダプター、LVM グループなどを管理できます。

VM：仮想マシン。

ボリューム：ゲストに割り当てたり、さらに多くのプールを作成するために使用したりできる、単一のストレージリソース。ブロックデバイス、raw ファイル、または特殊なフォーマット・ファイルをボリュームとして使用できます。

リファレンス

[1] Enomaly ECP アーキテクチャーのホワイトペーパー：<http://www.enomaly.com/Cloud-Hosting-Pr.466.0.html> (英語)

[2] Enomaly ECP SPE のデータシート：<http://www.enomaly.com/Cloud-Hosting-Pr.465.0.html> (英語)

[3] Enomaly ECP HAE のデータシート：<http://www.enomaly.com/Cloud-Hosting-Pr.465.0.html> (英語)

[4] 「Why the Intel® Xeon® Processor 5500 Series is the Ideal Foundation for Cloud Computing」：<http://communities.intel.com/docs/DOC-4213/> (英語)

[5] ソフトウェア業界におけるインテル® Xeon® 5500 番台の評価：<http://www.intel.com/business/software/testimonials/xeon5500.htm> (英語)

[6] 「Intel® in Cloud Computing」：<http://communities.intel.com/docs/DOC-4230/> (英語)

[7] Enomaly ECP/ インテル・テストベッドのインストールの詳細：http://enomaly.com/fileadmin/ICB/Enomaly_ECP_Intel_Testbed_Installation_Details.pdf (英語)

[8] インテル® AES-NI およびインテル® トラステッド・エグゼキュション・テクノロジー：<http://www.intel.co.jp/jp/technology/security/>

[9] インテル® インテリジェント・パワー・ノード・マネージャーおよびインテル® データ・センター・マネージャー：<http://software.intel.com/sites/datacentermanager/> (英語)

[10] Baidu POC：http://software.intel.com/sites/datacentermanager/intel_node_manager_v2e.pdf (英語)

[11] インテル® バーチャライゼーション・テクノロジー：<http://www.intel.co.jp/jp/technology/virtualization/> および <http://download.intel.com/jp/business/japan/pdf/321597-002JA.pdf>

クラウド・ソリューションの導入の詳細については、
<http://www.intel.com/software/cloudbuilder/> (英語) を参照してください。



免責条項

¹ インテル・プロセッサ・ナンバーはパフォーマンスの指標ではありません。プロセッサ・ナンバーは同一プロセッサ・ファミリー内の製品の機能を区別します。異なるプロセッサ・ファミリー間の機能の区別には用いません。詳細については、http://www.intel.com/jp/products/processor_number/ を参照してください。

² 出典：Black-Scholes* でのインテル® Xeon® プロセッサ X5680 とインテル® Xeon® プロセッサ X5570 のインテル社内での測定値。

³ 出典：SPECint*_rate_base2006 を使用して、インテル® Xeon® プロセッサ L5650 とインテル® Xeon® プロセッサ X5570 を比較した Fujitsu による性能測定。 <http://docs.ts.fujitsu.com/dl.aspx?id=4af74e10-24b1-4cf8-bb3b9c4f5f177389> を参照してください。

⁴ すべての条件下で絶対的なセキュリティを提供できるコンピューター・システムはありません。インテル® トラステッド・エグゼキューション・テクノロジー (インテル® TXT) は、インテルによって開発中のセキュリティ技術であり、このテクノロジーを利用するには、インテル® バーチャライゼーション・テクノロジー、インテル® TXT に対応したプロセッサ、チップセット、BIOS、Authenticated Code モジュール、インテル製または互換性のある Measured Virtual Machine Monitor (MVMM) を搭載したコンピューター・システムが必要です。さらに、インテル® TXT を利用するには、Trusted Computing Group によって定められた TPM v1.2 と、用途によっては、特定のソフトウェアも搭載している必要があります。詳細については、<http://www.intel.com/jp/technology/security/> を参照してください。

本資料に掲載されている情報は、インテル製品の概要説明を目的としたものです。本資料は、明示されているか否かにかかわらず、また禁反言によるとらえずにかかわらず、いかなる知的財産権のライセンスも許諾するものではありません。製品に付属の売買契約書『Intel's Terms and Conditions of Sale』に規定されている場合を除き、インテルはいかなる責任を負うものではなく、またインテル製品の販売や使用に関する明示または黙示の保証 (特定目的への適合性、商品適格性、あらゆる特許権、著作権、その他知的財産権の非侵害性への保証を含む) に関してもいかなる責任も負いません。インテルによる書面での合意がない限り、インテル製品は、その欠陥や故障によって人身事故が発生するようなアプリケーションでの使用を想定した設計は行われていません。

インテル製品は、予告なく仕様や説明が変更されることがあります。機能または命令の一覧で「留保」または「未定義」と記されているものがありますが、その「機能が存在しない」あるいは「性質が留保付である」という状態を設計の前提にしないでください。これらの項目は、インテルが将来のために留保しているものです。インテルが将来これらの項目を定義したことにより、衝突が生じたり互換性が失われたりしても、インテルは一切責任を負いません。この情報は予告なく変更されることがあります。この情報だけに基づいて設計を最終的なものとししないでください。

本書で説明されている製品には、エラッタと呼ばれる設計上の不具合が含まれている可能性があり、公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。最新の仕様をご希望の場合や製品をご注文の場合は、お近くのインテルの営業所または販売代理店にお問い合わせください。本書で紹介されている注文番号付きのドキュメントや、インテルのその他の資料を入手するには、1-800-548-4725 (アメリカ合衆国) までご連絡いただくか、<http://www.intel.com/jp/> を参照してください。

Intel、インテル、Intel ロゴ、Xeon、Xeon Inside は、アメリカ合衆国およびその他の国における Intel Corporation の商標です。

Microsoft、Windows、Windows ロゴは、米国 Microsoft Corporation および / またはその関連会社の商標です。

* その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。

インテル株式会社

〒100-0005 東京都千代田区丸の内 3-1-1

<http://www.intel.com/jp/>

©2011 Intel Corporation. 無断での引用、転載を禁じます。

2011年1月

323682-001JA

JPN/1101/PDF/SE/MKTG/ET