ベアメタル上のコンテナで 5G を最適化する

通信事業者がこのアーキテクチャを選んでいる理由

Red Hat 北米地域担当
エッジセールス
Tom Conklin (トム・コンクリン)

Red Hat プリンシパル
ソリューションアーキテクト
Sanjay Aiyagari
(サンジャイ・アイヤガリ)

「ベアメタル上のコンテナを採用し、最も新しく、最も革新的なサービスを実現することで、市場での競争力を強化できます。進化は、仮想マシンからコンテナに移行することでもたらされます。より多くのアプリケーションをより少ないインフラストラクチャで使えるようになるので、コストを削減し、サービスを短時間でデプロイしながら、顧客が必要とするセキュリティレベルを維持することができます」

Verizon、MEC および SDN 向け製品エンジニアリング担当取締役
Anoop Agrawal 氏

CSP がグローバル・クラウド・プロバイダーと同じ規模のメリットを得るためには、アプローチを変えなければなりません。仮想マシン (VM) からコンテナへと進化することによって、同等のパフォーマンス、効率、アジリティを実現できます。

エグゼクティブサマリー

通信ネットワークのクラウド移行に第二波が来ています。第一の波であったネットワーク機能仮想化 (NFV) は、要素マネージャーに対するレガシーなニーズをサポートしながら、アプライアンスベースのネットワーク要素からソフトウェアベースの要素へ移行することで、コスト低減を実現しました。現在、通信事業者 (CSP) は、クラウドネイティブなアーキテクチャとコンテナを採用し、効率、パフォーマンス、レジリエンシー (回復力)、セキュリティ、アジリティを向上させています。その際に選ばれているのが、仮想化のレイヤーを追加せず、ベアメタル上にコンテナをデプロイするアーキテクチャです。このようなアーキテクチャは、通信事業者のユースケースにおいて大きなメリットを提供します。

このホワイトペーパーでは、5G サービスをデプロイする際にベアメタルサーバー上のコンテナを使用するメリットを、仮想マシン (VM) 上のコンテナを使用した場合と比較しながら紹介します。

背景

ネットワーク機能がクラウドに移行し始めた頃、大手通信事業者に在籍していた一部の先見の明ある人々は、仮想マシン上にネットワーク機能をデプロイする段階を省略し、直接コンテナへ移行することを検討しました。Kubernetes の価値を理解し、初期の Kubernetes リリースに大きく貢献してきた Red Hat も、当初からこのアイデアを支持していました。しかし、業界全体の動きが OpenStack を推進したこと、そして当時のコンテナには通信ネットワーク用として使うにはいくつか不十分な点があったことから、そのような変化の基盤としては OpenStack® と VM が確立されました。ほとんどの CSP は、欧州電気通信標準化機構 (ETSI) の NFV アーキテクチャに従って仮想ネットワーク機能 (VNF) をデプロイし、現在のサービスを提供しています。当面の間、ネットワークと CSP の IT 領域では、仮想マシン上で実行されるレガシー・アプリケーションがなくなることはありません。しかし、今後新しいアプリケーションと 5G コンポーネントのほとんどは、コンテナを使用してデプロイされるでしょう。

テクノロジーの大変革が始まっています。レガシー・アプリケーションは、仮想マシンでの実行に適した旧来のモノリシックな形式から、マイクロサービスへと分割されつつあります。アジャイルと DevOps は、現在のアプリケーション開発・管理におけるベストプラクティスです。これらが最も効果的に機能するのは、アプリケーションがより小さなスタンドアローンのコンポーネントを使用して構築されている場合です。このアプローチでは、アプリケーションの他のコンポーネントに影響を与えることなく、各コンポーネントの機能と修正の開発およびデプロイを繰り返し行うことができます。CSP やそのベンダーは、毎年多くのアップグレードやパッチをサポートするために継続的インテグレーションおよび継続的デリバリー (CI/CD) を必要とすることが多いですが、アジャイル開発を実践することで、はるかに優れたサポートを提供できます。

VM の導入が要件となるケースは、時間の経過とともに減少しています。たとえば、VM を使用するメリットの 1 つに、さまざまなゲスト・オペレーティングシステムをサポートできることがありましたが、現在、このレベルの複雑さは不要となりました。Linux® がネットワーク・アプリケーションの標準オペレーティングシステムとなっていることに加え、複数のオペレーティングシステムをサポートするクラウドでは、セキュリティ脆弱性が検知された場合に必要な対策の複雑さが増してしまうためです。さらに、現在ではネットワーク機能とアプリケーションはステートフルではなくステートレスが標準となっているため、ネットワークストレージとの親和性もかつてほど大きな要件とはなりません。

総所有コスト (TCO) を最大 44% 削減[1]

Red Hat と ACG による調査で、専用の RAN テクノロジーにオープンな vRAN をデプロイすることにより、5G 導入の TCO を最大 44% 削減できることがわかりました。このコスト削減は、CSP が 5G をロールアウトに取り入れる上で重要な要因です。

通信業界における最も重要な変化の 1 つは、5G への進化です。これは、無線アクセスネットワーク (RAN) とコアの両方において言えます。[2] 5G により、CSP は、顧客やビジネスにとって最も適切な場所に基づいて、ネットワーク機能を複数の物理拠点に分散できるようになります。これによりパケットコアと音声機能を、パブリッククラウド、中央データセンター、各地域のデータセンター、さらには顧客の拠点にわたり分散することが可能になりました。また、RAN は、OpenRAN (O-RAN) Alliance および OpenRAN プロジェクト内でのコラボレーションと標準化によって進化し、プロプライエタリーのハードウェアではなく市販のサーバーでホストされる機能をサポートしています。コンポーネントは地理的に分散させることや、複数のベンダーから利用することが可能なほか、通信コアのコンポーネントやエンドユーザー向けに付加価値を提供するアプリケーションと、インフラストラクチャを共有利用できます。

コンテナはこのような進歩と相性がよく、ベアメタルにコンテナをデプロイすることで、CSP は大きなメリットを得られます。レガシー・アプリケーションの場合は、何らかの理由から VM にコンテナをデプロイすることもあるかもしれませんが、5G の場合、コンテナを VM の形式でデプロイして複雑さを増大させることは不要であり、非効率的です。

運用効率

通信ネットワークを仮想化する主なメリットの 1 つは、効率の向上です。従来、顧客に提供されるすべてのサービスには、テクノロジーの各層を管理する個別のグループによって維持される独自のテクノロジーセグメントに加えて、ネットワーク運用とカスタマーサポートがありました。サービスを構成するさまざまなネットワーク機能を同じクラウド・インフラストラクチャに配置することで、組織ごとに分断されていたこれらの層が排除されます。

当面の間、既存の機能向けのネットワークから仮想マシンがなくなることはないでしょう。しかし、5G コアや RAN などの新しい機能をコンテナにデプロイすると、大きなメリットが得られます。

VM からコンテナへの進化が、効率の低下になってはなりません。しかし、OpenStack と Kubernetes は 2 つの異なる専門技術であり、コンテナを VM に配置すると、既存の NFV アーキテクチャ内でレイヤーを単に置き換えるのではなく、リソースのレイヤーが追加されてしまいます。ネットワークのフットプリントを拡張して、パブリッククラウドのアセットと数千のリモートエッジサイトを含めると、複雑さが大きく増加します。コンテナではこの複雑さは Kubernetes によって対処されており、この環境で仮想マシンを維持すると、不要な複雑さと運用の非効率性が生じます。ベアメタルにデプロイされたコンテナであれば、あらゆる種類のクラウドにわたり共通の方法でサポートされますが、VM と VM をサポートする多様なプラットフォームでは異なります。その結果、コンテナ・プラットフォームと VM プラットフォームを並行してサポートするためにより多くの人員が必要となります。パブリッククラウドとプライベートクラウド用に異なるプラットフォームをサポートする場合は、さらに多くの人員が必要となります。理想としては、両タイプのクラウドに対して、単一のコンテナ・オーケストレーション・プラットフォームを使用すべきです。

分散型クラウドネイティブ・ネットワーク機能 (CNF) への移行に伴い、ライフサイクルの管理と保証に関して管理上の課題が生じる場合があります。1 つのアプリケーションを構成するマイクロサービス群は、必ずしも物理的に同一のサーバーや拠点上に存在するとは限りません。大幅に自動化されていない限り、ライフサイクル管理はかなりの手間となります。CSP とベンダーは、DevOps ツールチェーン、CI/CD 手法、そして現在は閉ループ保証を活用することで効率化に取り組んでいます。しかし、自動化を行うためには特定のスキルが必要であり、対応できる人材を確保するためのコストは高く、供給も不足しています。そのため、CSP はすべてのベンダーに対して、可能な限り共通の CI/CD パイプラインを使用するよう要求することが重要となります。

アップグレードとパッチは、統一された方法で自動的に配信、テスト、デプロイされるようにする必要があります。ネットワークが複雑化すれば、自動化資産を作成および更新し、自動化できない機能を手動で保守するために、より多くのリソースが必要になります。そのため、このような複雑化は、CSP が競争力を維持し、顧客の要求を満たすためにコスト削減を目指すうえでの妨げとなります。

[1] ACG Research、「Economic advantages of virtualizing the RAN in mobile operators' infrastructures」、Red Hat 後援、2019 年 9 月。

[2] 5G Americas、「5G and the cloud」、2019 年 12 月。

サービスのアジリティ

CSP は NFV によりサービスを俊敏化し、従来よりもはるかに迅速にサービスのデプロイや廃止を行えるようになりました。[3] さらに、5G の到来に伴い、CSP はサードパーティによるネットワークスライスの要求およびプロビジョニング可能となるよう、ネットワークの開放を計画しています。これにより、サードパーティは特化されたホールセール・アプリケーション用にネットワークスライスを利用できるようになります。この種のサービスは、ノースバウンド API (アプリケーション・プログラミング・インタフェース) を介して公開され、制御されたアクセスによりサードパーティにネットワークリソースを提供します。プロビジョニングのスピードは、顧客満足度にかかわる非常に重要な要素です。VM のスピンアップには、コンテナよりもはるかに長い時間がかかります。VM の場合、顧客はマウスを 2 回クリックしてスライスを要求できるかもしれませんが、それがさまざまなネットワークの場所にある多数の VM の形式でインスタンス化されるには何時間も待たなくてはならない可能性があります。しかし、サービスがコンテナベースであった場合、デプロイはほぼ瞬時に行われるため、この状況は大きく改善されます。

ベアメタル上のコンテナが実現するスピードは、将来的に、差別化されたエッジサービスの提供も可能とします。エンドユーザーが付加価値のあるサービスを要求した場合に、そのユーザーの付近のエッジノードにオンデマンドでデプロイすることもできます。ワークロード自体も同じエッジノード上で処理し続ける必要はなく、これらのノードを解放して、最も需要の高いアプリケーションだけホストすることが可能です。たとえば、移動の多いユーザーが、5G により可能となった高帯域幅の高信頼低遅延通信 (URLLC) アプリケーションを使用している場合、ユーザーの現在地に最も物理的に近いエッジサイトで処理を行うよう、アプリケーションに追跡させることも可能です。新しいエッジサイトに近づくと、アプリケーションは数秒でインスタンス化されます。これは、VM にデプロイされたコンテナでは実現できないメリットです。VM にコンテナをデプロイした場合、アプリケーションで使用する可能性のあるすべてのリソースをエッジで保有し、オンデマンドで VM をインスタンス化する必要があり、実用に耐えない長さの時間がかかるためです。

コンテナでサービスのアジリティを高めることで、より多くの収益を迅速に獲得し、廃止されたサービスが使用するリソースをより早く解放し、CSP が競争力を高めるために建設的なリスクを取ることができるようになります。[4] これらのメリットは、コンテナをベアメタル上にデプロイすることで、最も効果的に実現できます。

パフォーマンス

自然界と同様、通信ネットワークにおいても、進化はメリットをもたらすものでなくては意味がありません。進化は、問題の解決、ビジネス競争力の強化、存続の可能性の向上をもたらすべきです。コスト増加やパフォーマンス低下につながるような変化は、通常は受け入れられません。通信ネットワークには特定のパフォーマンス要件があり、この面から見ると VM にコンテナをデプロイするアプローチは退化と呼べます。

NFV では、仮想マシンによって生じる中断が、モバイルコアおよびインターネット・プロトコル・マルチメディア・サブシステム (IMS) アプリケーションにおける主要なハードルの 1 つとなっていました。まず、この影響により、サーバーの通常のパフォーマンスが最大 20% 低下する可能性があります。[5] より優れたパフォーマンスを必要とする CSP の場合、この影響により一部のアプリケーションを仮想化できなくなる可能性があります。とはいえ、シングルルート I/O 仮想化 (SR-IOV) やデータプレーン開発キット (DPDK) といったハードウェア・アクセラレーションのアーキテクチャや進化に重点的に取り組むことで、このパフォーマンスは大幅に向上しました。しかしコンテナと VM を組み合わせると、サービス停止の問題が再び浮上してきます。VM 上のコンテナは、現在ではコンピューティングに大幅な遅延を引き起こすことはなくなりましたが、VM のオーバーヘッドが余分にかかるため、ベアメタル上のコンテナと比較するとノードの入出力 (I/O) パフォーマンスは低くなります。この低下は、大規模な I/O トランザクションよりも小規模な I/O トランザクションでより顕著に現れます。通信ネットワークの音声およびデータトラフィックは、多くの場合、極めて断片化されており、小さなトランザクションで構成されています。

[3] Red Hat 事例、「Turkcell、Red Hat OpenStack ベースの NFV で統合通信クラウドを構築」、2020 年 4 月。

[4] Shirin Esfandiari、「Bringing 5G-enabled services to life calls for cloud-native operations」、DevOps.com、2019 年 8 月 20 日。

[5] Ming Liu ほか、「Understanding the virtualization "Tax" of scale-out pass-through GPUs in GaaS clouds: An empirical study」、IEEE.org、2015 年 2 月。

現在、最高水準のパフォーマンスを必要とするネットワーク機能は、中央処理装置 (CPU) の代わりに I/O を多用しており、VM 上のコンテナを使用してデプロイした場合はパフォーマンスが大幅に低下する可能性があります。この低下幅は 30% にまで及ぶ可能性があり、同じジョブを実行するためにより多くのコンテナが必要になります。[6] そして、VM 上のコンテナが増えることは、サーバーとコストの増加も意味します。

インフラストラクチャのメリット

NFV 以前、ネットワークハードウェアの使用率は、通常の負荷では非常に低いことがよくありました。冗長性はハードウェアで提供され、コストが増えました。スペアパーツを近くにストックしておくため、さらに費用が増加しました。容量はピーク使用時に合わせてモデル化され、収益性が非常に高い日も、需要が少なく収益性が低い日も、1 日のコストは同じでした。

理論的には、同一のインフラストラクチャ上で複数の VNF を仮想化した場合、使用率は大幅に向上します。ライフサイクル管理に高度なオーケストレーションを適用すると、冗長なハードウェアとスペアが不要になります。クラウドは、すべての VNF に共通の容量を提供し、各 VNF はその中で拡張や適合を行います。しかし実際には、VNF は多くの場合、本質的に異なるベンダー固有のハードウェアセグメントにデプロイされています。CSP はレガシーハードウェアと同じパフォーマンスと稼働時間を維持することをベンダーに求めたため、このような分離が必要でした。CSP に必要な 99.999% の可用性をサポートするためにクラウドリソースをプールすることはなく、セグメントは変わらずピーク容量を基準としてモデル化されました。また多くの場合、高可用性 (HA) を要求するアプリケーションでは、冗長なハードウェアセグメントがデプロイされました。このように、利用率の向上という可能性が実現されないことは珍しくありませんでした。そして多くの場合、その結果として、同一ネットワーク上に多種のテクノロジーセグメントが混在し、それぞれのベンダーから VM 管理用に提供された仮想インフラストラクチャ・マネージャー (VIM) が複数存在するような状況となっていました。

先進的なソフトウェア開発とライフサイクル管理手法により、5G コアと RAN コンポーネントは通常、コンテナで実行されるクラウドネイティブ機能として設計されています。第 3 世代パートナーシップ・プロジェクト (3GPP) で指定されたアーキテクチャにより、以前はモノリシックであった機能を、さまざまなベンダーやオープンソース・プロジェクトが提供するマイクロサービスにさらに分離することができます。CSP は、ベンダーがクラウド・インフラストラクチャを共有することを期待しており、クラウドネイティブのソフトウェア・アーキテクチャによって、NFV やその他の一般的なモノリシック・アプリケーションよりもベンダー・ソリューション間の共存の方が受け入れられやすくなっています。

コンテナはマイクロサービスのパッケージ化に非常に優れており、Kubernetes はマイクロサービスで構成されるアプリケーションのオーケストレーションを行います。コンテナが VM 内にデプロイされている場合、ストレージ、コンピューティング、およびメモリのリソースは各ゲスト・オペレーティングシステムに使用されます。これらのリソースは、最終的に各 VM にデプロイされるコンテナのニーズを認知することなく保有されます。その結果、レガシーネットワークと同様、使用率は低いままとなります。リソースは、ピーク時に必要な全コンテナをサポートできる量が保有されますが、そのように確保されたリソースにみあう需要が継続的に存在するわけではありません。ピークトラフィックに合わせた VM の場合、VM リソースの典型的な使用率はレガシーネットワークの場合と同様、約 20% となります。[7] 一方、ベアメタル上のコンテナをあるアプリケーションに合わせる場合、VM のような方法でリソースを保有することはなく、使用するコンピューティング・リソースは VM 上のコンテナの使用量の 20% にまで抑えられる場合もあります。このため、1 台のサーバーにより多くのコンテナを格納することができます。VM を使用した場合は使用率が低く、コンテナの密度が低下するため、追加ハードウェアの購入と管理による資本コストと運用コストが高くなります。

5G により実現するエッジアプリケーションにおいては、リソースの最適化が不可欠です。このようなリソースに含まれるものとして、ネットワーク、RAN、および低レイテンシーと予測可能な帯域幅を実現できるよう、顧客と近い地点にデプロイされたエンタープライズ・アプリケーションのワークロードが挙げられます。多くのエッジサイトでは、スペース上の制約または環境上の課題のため、追加のハードウェアを設置する余裕がありません。

[6] Guiseppe Lettieri ほか、「A study of I/O performance of virtual machines」、The British Computer Society、Vol. 61 No. 6、2018 年。

[7] Ming Liu ほか、「Understanding the virtualization "Tax" of scale-out pass-through GPUs in GaaS clouds: An empirical study」、IEEE.org、2015 年 2 月。

また、サイトの数によってサイト単位のコストの制約が生じ、総コストが即座に手に負えないほど増加する可能性があるため、多くの場合、それぞれが 1 台のサーバーに制限されます。仮想マシンを使う場合、エッジサーバー 1 台ごとに、ホスト OS のコストに加えて、すべてのゲスト OS のため多額のコストがかかります。ベアメタルの場合、必要なのはホスト OS のコストのみです。ベアメタル上にコンテナをデプロイすることで、トラフィックとサービスをより効率的に促進し、収益と利益率を強化できます。

セキュリティ

5G およびエッジネットワークをデプロイする CSP にとって、セキュリティの向上は、ベアメタルにコンテナをデプロイするにあたっての大きなメリットとなります。4G/LTE と NFV において、CSP がデプロイおよび管理するプライベートクラウド拠点の数は比較的少数でした。5G 時代では、複数のパブリッククラウドや、顧客拠点に近い、または顧客拠点内に存在する数千の小さなクラウドインスタンスなど、より分散したアーキテクチャの可能性が開かれます。さらに、顧客に付加価値サービスを提供するアプリケーションは、重要なネットワーク機能と同じクラウドインスタンスを共有することがあります。規模とマルチテナンシーを両立しようとする場合は、セキュリティを考慮すべきです。よくある間違いとして、「コンテナ化アプリケーションが別のアプリケーションに必要なリソースを使用しないように保護するためには VM が必要だ」という誤解があります。VM が 1 つのテナントのワークロードを別のテナントから安全に分離するというのも誤解です。実際には、セキュリティはオペレーティングシステムである Linux の機能であり、オーケストレーターである Kubernetes の機能ではありません。

VM は、クラウドノード上で互いから分離しあい、ワークロードが必要なリソースを互いから取得しないようにします。また、NFV およびモノリシック・アプリケーションに使用する場合は、実行されているアプリケーションの要件に合わせて構成されます。VM 上でコンテナをデプロイした場合でも、正しく処理しない場合、ベアメタル上のコンテナと同じように互いのリソースを奪い合う可能性があります。また、テナントのワークロードを個別の VM に分離すると、使用率が低下する可能性があります。これらの課題を解決するのが、一部の Linux ディストリビューションに付属するコンポーネントである Security-Enhanced Linux (SELinux) です。SELinux は、もともとは米国国家安全保障局 (NSA) によって開発されたセキュリティ・カーネル・モジュールであり、管理者は、オペレーティングシステムとノードのコンポーネントにアクセスするためのきめ細かな認可を制御することができます。セキュリティポリシーはノード自体に設定され、ノードにデプロイされた各コンテナは、その利益を保護するポリシーを実装します。コンテナが VM にデプロイされている場合でも、セキュリティを提供するために、ゲスト OS で SELinux を起動するべきです。ただし、VM はコンテナのセキュリティ保護に必須のものではありません。VM は、他の VM から自身を保護するだけです。VM のレイヤーを追加すると、コンプライアンスがより困難になるため、実際には CSP のネットワークのセキュリティに悪影響を与えることがあります。

もう 1 つのセキュリティ上の考慮事項は、CSP、ネットワークテナント、および規制機関によって決定されたセキュリティポリシーへの準拠です。ハードウェア、オペレーティングシステム、仮想インフラストラクチャ・マネージャー、アプリケーション、自動化スクリプト、およびその他のコンポーネントは、ベンダー、オープンソース・コミュニティ、または業界によって検知される潜在的なセキュリティ脅威を排除するために、継続的に監視と更新を行う必要があります。たとえば、5G ネットワークを運用して 5 年目だとしましょう。その時点では、複数の世代、場合によっては複数のベンダーのコンポーネントがネットワーク上に混在していることが考えられます。定期的なパッチ適用と、セキュリティ要件からの逸脱の修正を自動化することが必要です。VM は 1 台追加するごとに保守すべきゲスト OS も増えるため、コンプライアンスの維持が非常に複雑になります。

一部のコンテナは、セキュリティのための特定の SLA を持つサービスをサポートする場合があります。VM の形式でコンテナから物理ハードウェアを抽象化すると、セキュリティとパフォーマンスの調和が困難になります。Kubernetes には、コンテナが配置される特定のクラウドノードの概念がありません。ハードウェアとホスト・オペレーティングシステム間の関連付けをすべてのコンテナに提供できない場合、商用 (決済カード業界など) または医療 (HIPAA など) のコンプライアンスの対象となるワークロードのセキュリティを保証することは不可能です。コンテナをベアメタルにデプロイすると、セキュリティ・コンプライアンスの設定と保守が容易になります。

まとめ

4G/LTE と NFV において、大規模な通信ネットワークをサポートするために必要なプライベートクラウド・インスタンスの数は比較的抑えられていました。しかし、現在においては、5G が大きな変化をもたらしています。5G が新たに実現する予測可能な低レイテンシー、高帯域幅、分散アーキテクチャといった特徴の恩恵を受けたいと考える CSP は、ベアメタル上で実行されるコンテナに新しいネットワーク機能をデプロイすることで、より容易に成功を収められるでしょう。設備投資 (CAPEX) と運用費用 (OPEX) の削減を実現し、アジリティと競争力を高め、より小さなフットプリントでより優れたパフォーマンスを得ながら、ネットワーク・セキュリティを向上させることができます。

オープンソースは、イノベーション実現と問題解決の迅速化というメリットを提供します。これらは、コミュニティ全体が将来を見据えた課題の解決に注力しているために可能となる要素です。オープンソースを選ぶことで、CSP は特定のベンダーへのロックインを回避できます。Red Hat が提供する機能豊富なオープンソース・プロジェクトのディストリビューションには、使いやすさを向上させ、管理機能を自動化する、付加価値のある機能が備わっています。CSP は、以下のソリューションを使用して 5G ネットワークを構築できます。

CSP は Red Hat と連携することで、クラウドネイティブなネットワーク機能をベアメタル上で稼働させ、5G 展開から得られる価値を最大化できるよう取り組んでいます。

- Red Hat® OpenShift®
- Red Hat Ansible® Automation Platform
- Red Hat AMQ
- Red Hat 3scale API Management
- Quarkus の Red Hat ビルド (Kubernetes ネイティブの JavaTM ランタイム)

Red Hat は、世界中の多くの CSP による NFV へのネットワーク変革を支援してきました。OpenStack、Kubernetes、その他多数のオープンソース・プロジェクトへの主要なコントリビューターとして、Red Hat は通信ネットワーク・アーキテクチャをクラウドネイティブな形態へと進化させるための専門知識を豊富に有しています。さらに、Red Hat エコシステムパートナーが提供する認定済みのネットワーク機能は、選択肢を提供するとともに、安心してデプロイできます。詳細は、Red Hat の通信ソリューションのページをご覧ください。

アジア太平洋 +65 6490 4200
apac@redhat.com
オーストラリア 1 800 733 428
インド +91 22 3987 8888
インドネシア 001 803 440 224
日本 0120 266 086
03 5798 8510
韓国 080 708 0880
マレーシア 1 800 812 678
ニュージーランド 0800 450 503
シンガポール 800 448 1430
中国 800 810 2100
香港 800 901 222
台湾 0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

Red Hat について

エンタープライズ・オープンソースソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、新規および既存 IT アプリケーションの統合、クラウドネイティブ・アプリケーションの開発、Red Hat が提供する業界トップレベルのオペレーティングシステムへの標準化、複雑な環境の自動化、セキュリティ保護、運用管理を支援します。受賞歴のあるサポート、トレーニング、コンサルティングサービスを提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーです。クラウドプロバイダー、システムインテグレーター、アプリケーションベンダー、お客様、オープンソース・コミュニティの戦略的パートナーとして、Red Hat はデジタル化が進む将来に備える企業を支援します。

O-F25719