

BladeSymphony ファームウェアの開発(5) BS2000 RHEL KVM on LPAR ユースケースの提案

田島 幸恵[†]

(株) 日立製作所 横浜研究所[†]

1 はじめに

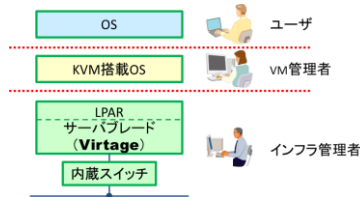
1 台の計算機上で複数の計算機環境を稼働させる方式には LPAR 方式と VM 方式があり、各々堅牢性と柔軟性という異なる優位点を持つ。

両優位点を活用する機構として、LPAR 方式で計算機リソースを論理分割した環境上に VM 方式を用いた計算機環境 (VM) を構築する階層制御機構が考えられる。本制御機構を用いることで堅牢性と柔軟性を同時に満たすことが可能となるが、VM と物理環境の間の層数が増えることからリソース管理が複雑になることが予想される。

一例として、あるユースケースを前提とし、VM で保証されているように見えるネットワークの独立性を物理環境で維持する際に想定される課題を示し、解決案を提案する。

2 RHEL KVM on LPAR のネットワーク構成

RHEL KVM on LPAR 環境例を以下の図に示す。本環境はインフラ管理者、VM 管理者、ユーザの 3 種類のプレイヤーによって管理・利用される。



インフラ管理者は、内蔵スイッチやサーバブレード、サーバブレード上の仮想化機構である Virtage, LPAR の管理を行なう。

VM 管理者は LPAR 上にインストールされた OS の管理を行なう。VM 管理者は、LPAR のリソースを効率的に利用するために仮想化機構 KVM を LPAR 上の OS にインストールすることができる。また、DBMS 等の性能要件が厳しいソフトウェアを稼働させるために LPAR 上に非仮想化環境の OS をインストールすることもできる。

ユーザは、VM 管理者によって作成された計算

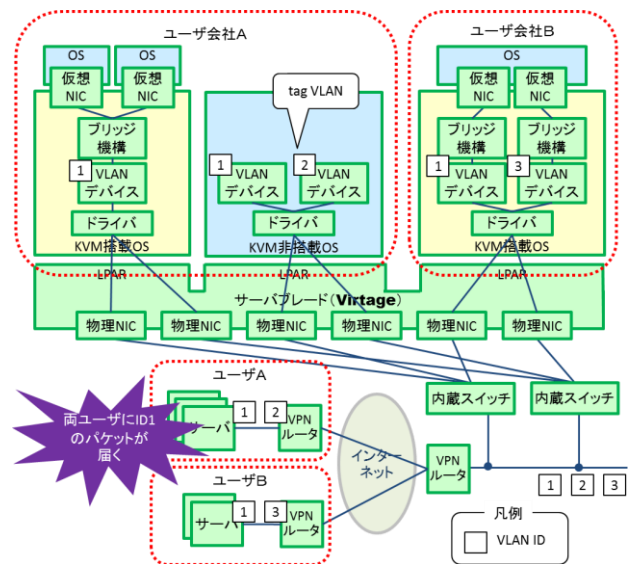
機環境 (VM) を使用する。

各々のプレイヤーの操作できるリソースは制限されている。例えば、VM 管理者はインフラ管理者の操作可能リソースである LPAR への (物理) デバイス割り当てを変更することはできない。また、同様にインフラ管理者も VM 管理者の操作可能リソースである (仮想) デバイスの割り当ての設定を変更することはできない。

3 仮想化環境貸し出しビジネスモデル

RHEL KVM on LPAR にはいくつかのユースケースがある。本論文では、このうちの一つである、KVM 環境全体を特定のユーザに貸し出す「仮想化環境丸ごと貸し」ビジネスの形態を想定する。

本形態では以下の図に示すように、インフラ管理者であるクラウドベンダが 1 台のサーバ上に複数の LPAR を構築し、ユーザ会社に LPAR 単位で貸し出しを行なう。



LPAR を貸与されるユーザ会社には、VM 管理者とユーザが存在する。VM 管理者は、LPAR に RHEL KVM (または RHEL) をインストールし計算機環境を構築する。この際用途に応じて VLAN でネット

[†] Sachie Tajima, Yokohama Research Laboratory, Hitachi, Ltd.

ワークを分割することで、ユーザにセキュアなネットワーク環境の提供を試みる可能性がある。例えば2つのVLANを作成し、VLAN 1はOA用、VLAN2はバックアップ用、と割り当てるかもしれない。

VLAN IDは各ユーザ会社が独自に設定して利用する値である。この値はVM管理者が設定するものでありインフラ管理者からは操作不能である。そのため図のように、ユーザ会社が各々設定したVLAN IDが衝突してしまう可能性がある。VLAN IDが衝突した場合、あるユーザ会社の packets が別のユーザ会社から受信可能になるという情報漏洩問題が発生する。つまり、ユーザ会社からは維持されているように見えるネットワークリソースの独立性が実際には侵される可能性がある。

クラウドベンダがユーザ会社毎に使用するIDを指定することで衝突の回避は可能である。しかしこれはユーザ会社の利便性を下げる方式であり、サービスとして提供するには困難が伴う。

4 独立性を保証するネットワーク構成

本論文では、ユーザ会社 (VM 管理者) が VLAN (タグ VLAN) を用いて用途に合わせてネットワークを分割することを想定している。

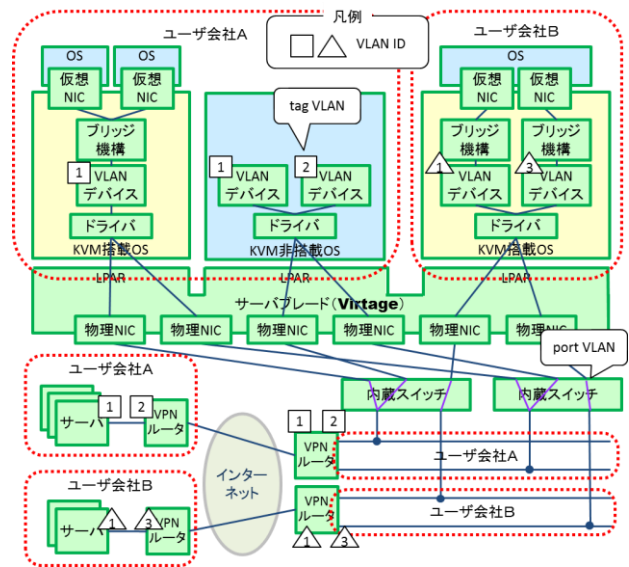
インフラ管理者には、VM 管理者が操作するリソースであるタグ VLAN 情報を操作することはできない。そのため、インフラ管理者は別の方式を用いてユーザ会社毎にネットワークを分割する必要がある。

分割方式としては、例えばスイッチにおいて二重タギングを用いる方式と、ポート VLAN を用いる方式が挙げられる。

二重タギングには、自由度の高い構成を組むことができるというメリットがある。一方で対応しているスイッチが少ないこと、パケットサイズが拡張するために経路上の全てのスイッチが拡張サイズのパケットを許容する必要があることがデメリットとして挙げられる。

ポート VLAN には、多くのスイッチが対応しているというメリットと、分割できるネットワークの数がスイッチの持つポート数に制限されるため構成の自由度が低いというデメリットが挙げられる。

構成の自由度が低いというデメリットはあるが、一般的なスイッチでも環境を構築できるというメリットを重視し、ポート VLAN を用いてのネットワーク分離を検討する。



ポート VLAN を用いてネットワークを分離した様子を上図に示す。本方式により、ユーザ会社毎に独立性を保証したネットワーク構成が構築可能と考えられる。

5 おわりに

本論文では計算機環境を階層制御する場合、階層毎にプレイヤーを設けることでリソースの管理が複雑になることの一例を示した。

本問題を解決する方式として、VM 管理者がタグ VLAN、インフラ管理者がポート VLAN の設定を行なう方式を検討した。これにより、各プレイヤーの意図通りの環境構築が実現できると考えられる。

しかし本方式には構成の自由度に制限があるというデメリットが存在する。本デメリットの解消が課題である。

本課題を解決するため、XVLAN や OpenFlow といった機構の利用を検討したい。

参考文献

- [1] 服部直也他, 2 種類の仮想化方式を共存させる仮想 VT-x 方式の提案, 2010 年電子情報通信学会 総合大会
- [2] 水野和彦他, 2 段仮想化構成のユースケース提案と評価, 2012 年電子情報通信学会 総合大会
- [3] 服部直也他, 2 段仮想化構成のメモリ性能改善と評価, 2012 年電子情報通信学会 総合大会