6D-3

仮想マシンのオペレーショントレースに関する考察

高田　慎也　　竹内　格　　石本　英隆　　中原　慎一
NTT 情報流通プラットフォーム研究所
takada.shinya@lab.ntt.co.jp

1.はじめに

今後成長していくクラウドでは様々な仮想環境プラットフォームを一元的に管理し、仮想マシンの整理をする必要性が生じる。これを実現する上で、仮想環境下で、誰が何をしたかという、いわゆる 4W1H1R の証跡ログを管理することでセキュリティを高めることが必要となってきている。

証跡ログの管理対象としては、仮想環境の運用者が行ったオペレーションのトレース、仮想環境上のコンテンツの流通のトレース、仮想環境で提供されるサービスのトレースと大きく 3 つに分類される[1]、本稿では特に仮想環境でのオペレーションのトレースに注目し、4W1H1R の証跡ログを取得する方法について検討する。

2.オペレーショントレース要件

オペレーショントレースでは、説明責任を果たすため以下の 4W1H1R の項目を満たす証跡ログを仮想環境でのすべてのオペレーションについて取得することが必要である。

・操作分類（出力契機）：What
・操作日時：When
・操作者：Who
・操作対象ホスト名：Where
・操作対象：What
・操作による変更内容：How
・操作結果の出力有無：Result

また、1 章で述べたとおりクラウドにおいては、マルチベンダの仮想環境を用いた混合運用も想定されるため、複数の仮想環境実装（VMware, KVM,Xen）においても同様に、各オペレーションで上記項目を満たす証跡ログを収集することが必要となる。

3.仮想環境からﾃﾞﾌｫﾙﾄ出力されるログの調査

既存の仮想環境での運用者の手順を想定して、オペレーションに対してデフォルトで出力される項目の有無を調査した。評価対象の仮想環境は、VMware の場合、ESXi が出力するログを対象とした。表 1 が VMware についての調査結果である。評価対象のログはデフォルトで重要度が info 以上である Syslog を対象とした。

多くのオペレーションで操作者や操作対象が欠落し、ログから誰が操作したかを判別できないことが分かった。また一部のリソース変更では、変更内容を取得することができないことも分かった。

他にも vCenter や KVM を調査した結果、既存の仮想環境からデフォルト出力されるログは、4W1H1R の証跡ログを取得し、オペレーションをトレースするとい

表 1 VMware ESXi においてデフォルトで取得できる情報

操作内容	出力項目						
	操作分類（出力契機）	操作日時	操作者	操作対象ホスト名	操作対象	操作による変更内容	操作結果
ログイン	○	○	○	×	−	−	○
ログアウト	○	○	○	×	−	−	○
仮想マシンの新規作成	○	○	×	○	○	−	○
仮想マシンの名前変更	○	○	×	×	○	○	○
CPUリソースの変更	×	○	×	○	×	×	○
メモリリソースの変更	×	○	×	○	×	×	○
ディスクリソースの変更	×	○	×	○	○	○	○
仮想マシンの移動	○	○	○	×	○	○	○
仮想マシンの複製	○	○	○	×	○	○	○
仮想マシンの削除	○	○	○	×	○	−	○
仮想マシンの起動	○	○	×	○	○	−	○
仮想マシンの停止	○	○	×	○	○	−	○
ESXiの停止	○	○	×	○	−	−	○

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

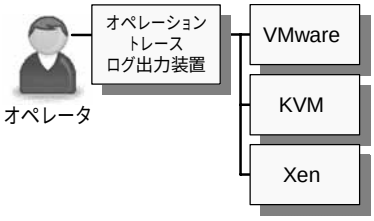

図 1　証跡ログ補完アーキテクチャ

う観点からは不十分なものであることが分かった。

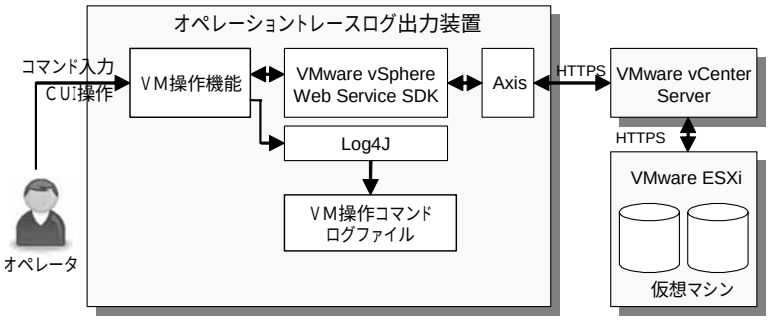

図 2　オペレーショントレースログ出力装置の構成

4.仮想環境のｵﾍﾟﾚｰｼｮﾝﾄﾚｰｽﾛｸﾞ出力ｺﾏﾝﾄﾞの実装

前章で明らかとなった、ログの未出力項目を補完するために、図 1 に示すような証跡ログ補完アーキテクチャを想定し、今回 VMware について vSpere Web Service SDK を使用して、補完項目を出力するオペレーションコマンドを作成した。コマンドは CUI ベースとし、対象オペレーションは、仮想マシンの移動（vMotion）を除く、表 1 に示したすべてのオペレーションとした。仮想マシンの移動を対象外としたのは、実装に使用した vSphere が仮想マシンの移動に対応していないためである。

図 2 に作成したオペレーショントレースログ出力装置の構成を示す。ログ出力は汎用性を考慮し Log4J を使用することとした。また仮想マシンの複製コマンドを実現するために、vCenter Server を介して ESXi にアクセスする構成とした。考案したオペレーショントレースログ出力装置では、VM 操作機能でセッションを管理することで、表 1 で欠落していた情報の補完を行う。

5.実装結果の評価

作成したコマンドのログ出力結果を図 3 に示す。各オペレーションに対して、デフォルトでは出力されなかった項目が、作成したコマンドのログでは出力されていることが分かる。これにより、作成したコマンドを用いて、仮想マシンのオペレーショントレースが可能な、4W1H1R の証跡ログを取得することが可能であることを実機で検証することができた。これにより、2 章であげた説明責任を VMware を用いた仮想環境については、満たすことができ、解決できることがわかった。

作成したコマンドの処理時間を表 2 に示す。処理時間は概ね十数秒かかり、ＯＳがインストールされている仮想マシンの複製には、容量に応じ 2 分近くかかることが分かった。作成したコマンドの処理時間が概ね十数秒かかっている原因としては、システムの一部(vCenter)を仮想環境で動作させていることによる処理時間が支配的であり、今回の実装の影響は軽微である。

表 2　各コマンドの処理時間

処理内容	平均処理時間（3回の平均値）
ログイン	12．14秒
ログアウト	11．17秒
VM新規作成	21．60秒
VM削除	12．44秒
VM名前変更	12．81秒
CPUリソース変更	13．16秒
メモリリソース変更	13．51秒
ディスクリソース変更	14．81秒
VM複製	117．37秒
VM起動	14．03秒
VM停止	13．94秒
ESXi停止	13．16秒

6.今後の予定

今後、システムを実環境で再構築した上で性能評価を行っていきたい。また、対象とする仮想環境の実装を増やす(例えば KVM, Xen)ことも検討したい。

7.参考文献

[1]Shinichi Nakahara et al, A study on the requirements of accountable cloud services and log Management: B-7-1 APSITT 2010

```
2010-08-03 15:52:52,737  INFO - [STR=2010/08/03 15:52:42 240;END=2010/08/03 15:52:52 735;OPR=Login;USR=tester1;HST=129.60.19.31;BEF=;AFT=;RST=OK]
2010-08-03 15:53:22,342  INFO - [STR=2010/08/03 15:53:09 898;END=2010/08/03 15:53:22 340;OPR=RenameVM;USR=tester1;HST=129.60.19.31;BEF=test1;AFT=test2;RST=OK]
2010-08-03 15:55:42,776  INFO - [STR=2010/08/03 15:55:29 240;END=2010/08/03 15:55:42 774;OPR=ModifyCPU;USR=tester1;HST=129.60.19.31;BEF=test2;1;AFT=test2;2;RST=OK]
2010-08-03 15:56:31,120  INFO - [STR=2010/08/03 15:56:18 552;END=2010/08/03 15:56:31 118;OPR=ModifyMemory;USR=tester1;HST=129.60.19.31;BEF=test2;256;AFT=test2;512;RST=OK]
2010-08-03 15:58:23,121  INFO - [STR=2010/08/03 15:58:09 212;END=2010/08/03 15:58:23 119;OPR=ModifyDisk;USR=tester1;HST=129.60.19.31;BEF=test2;1;AFT=test2;5120;RST=OK]
2010-08-03 16:00:30,758  INFO - [STR=2010/08/03 16:00:17 634;END=2010/08/03 16:00:30 756;OPR=StartVM;USR=tester1;HST=129.60.19.31;BEF=;AFT=test2;RST=OK]
2010-08-03 16:01:56,502  INFO - [STR=2010/08/03 16:01:29 022;END=2010/08/03 16:01:56 501;OPR=StopVM;USR=tester1;HST=129.60.19.31;BEF=;AFT=test2;RST=OK]
2010-08-03 16:02:29,759  INFO - [STR=2010/08/03 16:02:19 314;END=2010/08/03 16:02:29 757;OPR=Logout;USR=tester1;HST=129.60.19.31;BEF=;AFT=;RST=OK]
```

図 3 作成したコマンドのログ出力結果

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.