

GMO クラウド Private

Zabbix

エージェントインストール手順書

[Linux & Windows]

■更新履歴

バージョン	日付	内容
1.0	2017/10/13	初版作成

はじめに

本書は、GMO クラウド Private サービスで提供している監視復旧オプションのクライアント・サーバー (Linux、Windows) に Zabbix エージェントをインストールする手順についてのマニュアルです。

本書では Zabbix エージェントを導入するに当たって必要となる下記オペレーションについて記載しています。

- Linux 環境へのエージェントインストール
- Windows 環境へのエージェントインストール

本書は、当社の許諾なく複製または第三者への使用を禁止する。

サービス運用部 SE グループ

目次

1	Linux サーバーへのインストール	5
1.1	Yum を利用したインストール	5
1.2	メディアからのインストール(外部疎通がない環境)	7
1.3	Zabbix エージェントの設定ファイルを修正	8
1.4	Zabbix エージェント 起動設定	8
1.5	スタティックルート (静的経路) 追加設定	9
1.6	ファイアウォール設定変更	10
1.7	sudouser の設定	10
2	Windows サーバーへのインストール	11
2.1	WEB ブラウザからパッケージの入手	11
2.2	メディアからのインストール(外部疎通がない環境)	12
2.3	パッケージのインストール	12
2.4	Windows ファイアウォールの設定	16
2.5	スタティックルート (静的経路) 追加設定	20
3	VMware vCloud Director からの CD マウント	21
3.1	仮想サーバーへのメディアの挿入	21
3.2	仮想サーバーでのマウント/アンマウント操作	22
3.3	仮想サーバーからのメディアの取り外し	22

1 Linux サーバーへのインストール

本項ではLinux サーバー向けの「yum を利用したインストール方法」及び、「ISO イメージからのインストール方法」を説明しています。

1.1 Yum を利用したインストール

外部疎通が出来ない環境などで、ISO イメージを利用する場合次の項「1.2 メディアからのインストール(外部疎通がない環境)」よりご覧ください。

監視対象 VM がネットワークに接続されている場合、Zabbix のリポジトリを登録し、リポジトリからパッケージを指定し、インストールを行います。

① Zabbix リポジトリの登録

以下のコマンドで、RedhatEnterprise6 64bit の Zabbix リポジトリの登録を行います。

```
# rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/6/x86_64/zabbix-release-3.0-1.el6.noarch.rpm
```

他のバージョンのパッケージについては、下表の URL をご参照ください。

RHEL5 CentOS5	32bit	http://repo.zabbix.com/zabbix/3.0/rhel/5/i386/zabbix-release-3.0-1.el5.noarch.rpm
	64bit	http://repo.zabbix.com/zabbix/3.0/rhel/5/x86_64/zabbix-release-3.0-1.el5.noarch.rpm
RHEL6 CentOS6	32bit	http://repo.zabbix.com/zabbix/3.0/rhel/6/i386/zabbix-release-3.0-1.el6.noarch.rpm
	64bit	http://repo.zabbix.com/zabbix/3.0/rhel/6/x86_64/zabbix-release-3.0-1.el6.noarch.rpm
RHEL7 CentOS7	64bit	http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm

② パッケージの確認

リポジトリを検索して、zabbix パッケージが取得可能であることを確認します。

```
# yum search zabbix

出力例
# yum search zabbix
読み込んだプラグイン:fastestmirror, security
Determining fastest mirrors
epel/metalink | 5.3 kB 00:00
 * base: www.ftp.ne.jp
 * epel: ftp.kddilabs.jp
 * extras: www.ftp.ne.jp
 * updates: www.ftp.ne.jp

===== N/S Matched: zabbix
=====
python-pyzabbix.noarch : PyZabbix is a Python module for working with the Zabbix
API
uwsgi-stats-pusher-zabbix.x86_64 : uWSGI - Zabbix Stats Pusher for uWSGI
zabbix-agent.x86_64 : Zabbix Agent

省略

zabbix22.x86_64 : Open-source monitoring solution for your IT infrastructure
Name and summary matches only, use "search all" for everything.
```

③ Zabbix エージェントをインストール

yum コマンドにて Zabbix エージェントのインストールを行います。

```
# yum -y install zabbix-agent

出力結果
(1/2): zabbix-3.0.8-1.el6.noarch.x86_64.rpm
| 161 kB 00:01
(2/2): zabbix-agent-3.0.8-1.el6.noarch.x86_64.rpm
| 173 kB 00:00

-----

合計
124 kB/s | 334 kB 00:02
警告: rpmts_HdrFromFdno: ヘッダ V4 DSA/SHA1 Signature, key ID 79ea5ed4: NOKEY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX
Importing GPG key 0x79EA5ED4:
Userid : Zabbix SIA packager@zabbix.com
Package: zabbix-release-3.0-1.el6.noarch (installed)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX
rpm_check_debug を実行しています
```

省略

インストール:

```
zabbix-agent.x86_64 0:3.0.8-1.el6.noarch
```

依存性関連をインストールしました:

```
zabbix.x86_64 0:3.0.8-1.el6.noarch
```

完了しました!

上記が問題なく完了しましたら、「1.3 Zabbix エージェントの設定ファイルを修正」にお進みください。

1.2 メディアからのインストール(外部疎通がない環境)

本項では ISO イメージをマウントし ISO イメージ内のパッケージを指定しインストールする手順を説明しています。

※「1.1 Yum を利用したインストール」を実施済みの方は本項を実行する必要はありません。

- ① 最初に、ISO イメージのマウントを「3 VMware vCloud Director からの CD マウント」の手順より実施します。
- ② /mnt/cdrom に移動して以下のコマンドを実施してください。

CentOS5 64bit の Zabbix エージェントのインストールを行います。

```
# rpm -ivh zabbix-agent-3.0.7-1.el5.i386.rpm
```

他のバージョンのパッケージについては、下表をご参照ください。

RHEL5	32bit	rpm -ivh zabbix-agent-3.0.7-1.el5.i386.rpm
CentOS5	64bit	rpm -ivh zabbix-agent-3.0.8-1.el5.x86_64.rpm
RHEL6	32bit	rpm -ivh zabbix-agent-3.0.8-1.el6.i686.rpm
CentOS6	64bit	rpm -ivh zabbix-agent-3.0.8-1.el6.x86_64.rpm
RHEL7	64bit	rpm -ivh zabbix-agent-3.0.7-1.el7.x86_64.rpm
CentOS7		

- ③ インストール完了後、ISO イメージのアンマウントを「3 VMware vCloud Director からの CD マウント」の手順より実施します。

1.3 Zabbix エージェントの設定ファイルを修正

Zabbix エージェントを有効に機能させるためには、設定ファイルの修正が必要となります。

vi エディタ等を利用し zabbix-agent の設定ファイル「/etc/zabbix/zabbix_agentd.conf」内にある下記の箇所を編集し修正追記します。

① 変更前の状態

```
Server=127.0.0.0
ServerActive=127.0.0.0
Hostname=Zabbix server
# EnablesRemoteCommands=0
```

② 変更後の状態

```
Server=192.168.251.241
ServerActive=192.168.251.241
Hostname=登録ホスト名をここに記入
EnableRemoteCommands=1
```

③ Zabbix エージェントのサービスを再起動します。

```
CentOS6 以前の Linux)
# /etc/init.d/zabbix-agent restart
```

```
CentOS7)
# systemctl restart zabbix-agent
```

1.4 Zabbix エージェント 起動設定

Zabbix エージェントを起動時に動作する設定をします。

① サーバー再起動時に zabbix エージェントが自動起動するように設定します。

```
CentOS6 以前の Linux)
# chkconfig zabbix-agent on
```

```
CentOS7)
# systemctl enable zabbix-agent
```

② 登録確認

CentOS7 以前の Linux) 「2:」～「5:」が「on」となっていることを確認

```
# chkconfig --list zabbix-agent
zabbix-agent    0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

CentOS7) 「enabled」の応答を確認

```
# systemctl is-enabled zabbix-agent
enabled
```

1.5 スタティックルート（静的経路）追加設定

弊社の監視サービスは「ローカルネットワーク」を経由し「監視サーバー」と「監視対象 VM」が通信を行います。そのためスタティックルートの設定が必要となります。

事前に設定完了通知に記載されているローカルネットワークをご確認ください。

① スタティックルートの追加

```
# ip route add 192.168.251.241/32 via ローカルNWゲートウェイIP
```

例) `ip route add 192.168.251.241/32 via 10.1.4.254 dev eth1`

恒久的に設定するために以下のファイルを作成し記述を追記します。

```
# vi /etc/sysconfig/network-scripts/route-[プライベートNWのI/F名]
```

```
192.168.251.241/32 via ローカルNWゲートウェイIP
```

例) `192.168.251.241/32 via 10.1.4.254`

② 設定確認

下記の出力例のように設定が反映されていることを確認します。

```
# netstat -rn|grep 192.168.251.241
```

出力例

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS Window	irrt	Iface
192.168.251.0	10.1.4.254	255.255.255.0	UG	0 0	0	eth1

Zabbixサーバーへpingを実施しZabbix監視サーバーへの疎通を確認します

```
# ping 192.168.251.241
```

1.6 ファイアウォール設定変更

OS で通信制限をしていない場合はこちらの項を実施する必要がございません。

Zabbix 監視ではポート「10050」を利用します。

※以下の手順は 10050 番ポートの通信を許可する設定例となります。

設定方法の詳細につきましては iptables の man ページ等をご確認ください。

1.6.1 iptables 利用時

```
# iptables -I INPUT -p tcp -m tcp --dport 10050 -j ACCEPT
```

設定を恒久的に保存

```
# service iptables save
```

設定反映

```
# service iptables restart
```

1.6.2 firewalld 利用時

Firewalld を利用の場合は以下の設定を実施します。

```
# firewall-cmd --add-port=10050/tcp --zone=public --permanent
```

```
# systemctl restart firewalld
```

個別にお客様がポート監視を申し込まれている場合は同様に設定を追加してください。

1.7 sudouser の設定

この項はプロセス再起動をご利用されるかたのみ設定を実施します。

再起動コマンドの実行は OS 上の zabbix ユーザーが実行する仕組みとなっているため、zabbix ユーザーに sudo の設定を行います。

① sudoers を編集

```
# visudo
```

CentOS6 以降) 行を追記

```
zabbix ALL=(root) NOPASSWD: ALL
```

CentOS5 以前) 設定をコメントアウト

```
Defaults    requiretty
```

↓ コメントアウト

```
#Defaults    requiretty
```

行を追記

```
zabbix ALL=(root) NOPASSWD: ALL
```

2 Windows サーバーへのインストール

本項では Windows 版のインストーラーを入手しインストールを実施、その後ファイアウォール設定と静的経路の設定をする方法を記述します。

2.1 WEB ブラウザからパッケージの入手

監視対象 VM がインターネット環境の利用が可能な場合はインストーラーを WEB サイトからダウンロードします。

外部接続が出来ない環境などで、ISO イメージを利用する場合には次項「2.2 メディアからのインストール (外部疎通がない環境)」からご覧下さい。

以下の URL からインストーラーをダウンロードします。

<http://www.suiviperf.com/zabbix/>

または

<http://www.suiviperf.com/zabbix/old>

3.0.x の安定版 (3.0.x 以降推奨) をクリックし、MSI ファイルをダウンロードします。

例)

32bit	zabbix_agent-3.0.7_x32.msi
64bit	zabbix_agent-3.0.7_x64.msi

ダウンロードが完了しましたら「2.3 パッケージのインストール」の項にお進みください。

2.2 メディアからのインストール(外部疎通がない環境)

ISO イメージをマウントし ISO イメージ内のパッケージを指定しインストールする手順をこの項では説明します。

- ① ISO イメージのマウントを事前に「3 VMware vCloud Director からの CD マウント」の手順より実施します。

- ② ISO イメージをマウントしたら以下のパッケージを確認し実行します。

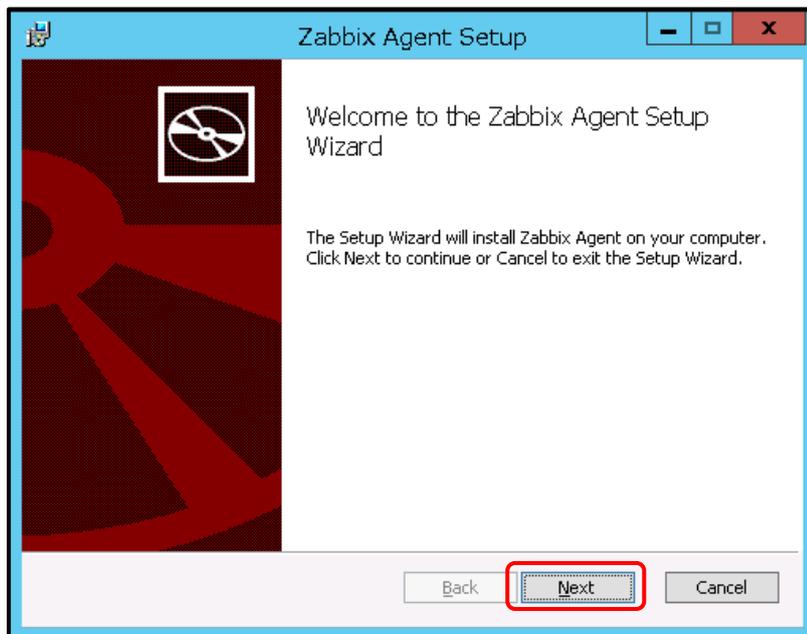
※初期設定の Windows では自動起動します。

32bit	zabbix_agent-3.0.7_x32.msi
64bit	zabbix_agent-3.0.7_x64.msi

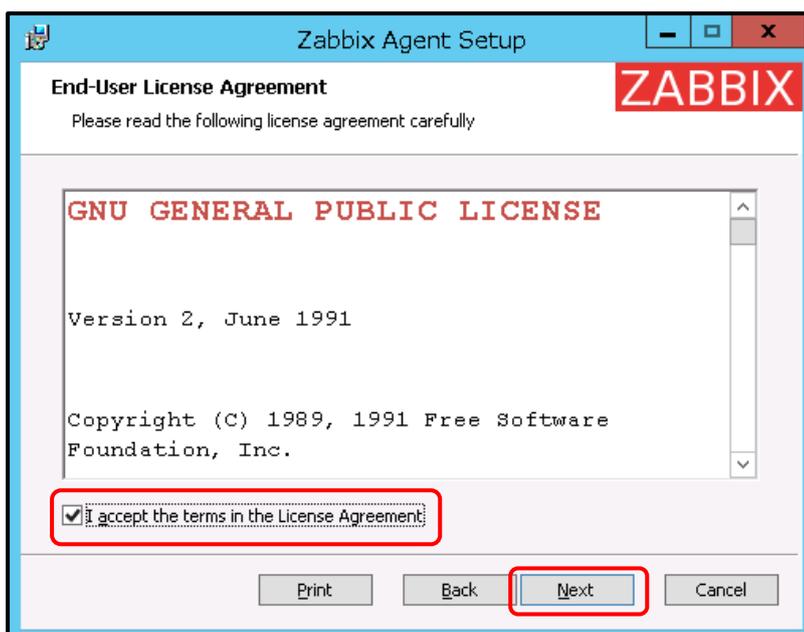
2.3 パッケージのインストール

Windows 上の MSI ファイルを実行し Zabbix エージェントをインストールします。

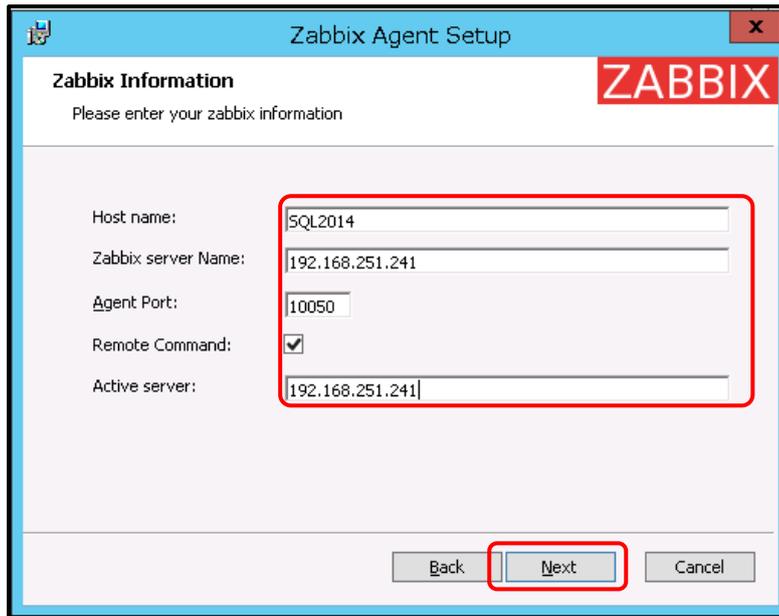
- ① OS に合った MSI インストーラーを実行します。
- ② ウィンドウ下部の「Next」を押下します。



- ③ 規約を承諾にチェックを入れて「Next」を押下します。



④ 監視対象の情報を記入し次へ「Next」を押下します。



【Host name】
監視設定ヒアリングシート参照

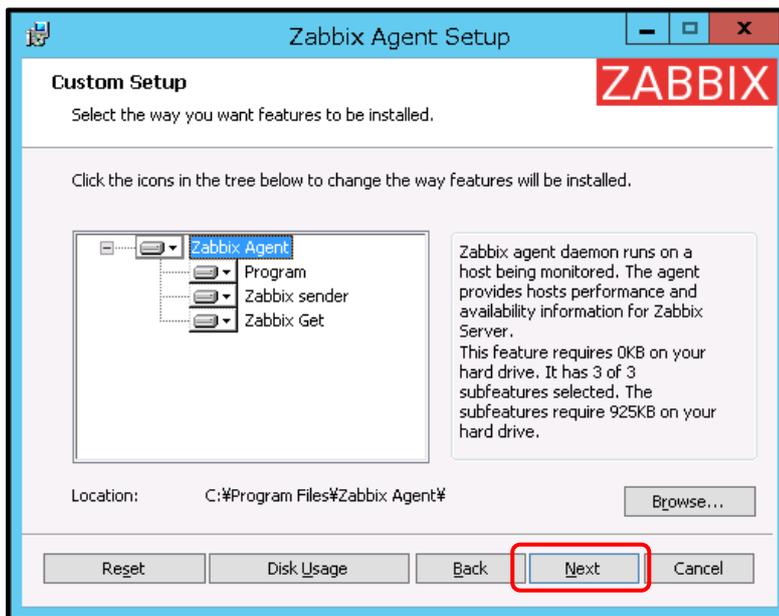
【Zabbix server Name】
192.168.251.241

【Agent Port】
10050

【Remote Command】
チェックを入れる

【Active server】
192.168.251.241

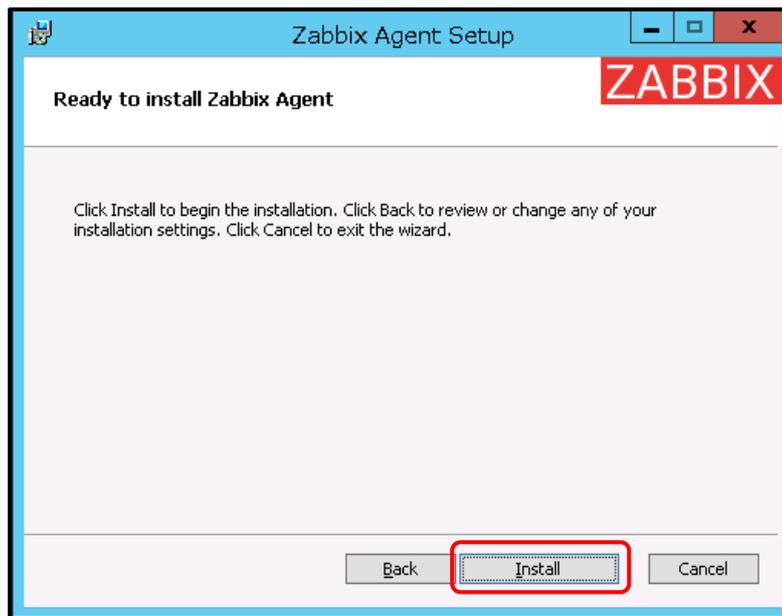
⑤ インストールディレクトリは、デフォルトのままを次へ「Next」を押下します。



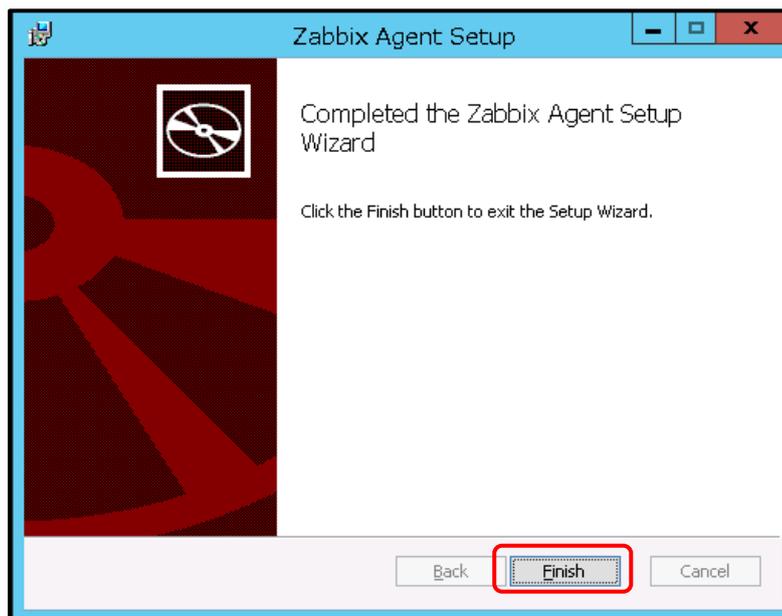
※32bit/64bit で下表のディレクトリがデフォルトで選択されます

32bit	C:\Program Files(x86)\Zabbix Agent
64bit	C:\Program Files\Zabbix Agent

- ⑥ 画面下部の「Install」を押下してインストールを実行します。



- ⑦ インストールが完了を確認後、【Finish】を押下します。



2.4 Windows ファイアウォールの設定

OS でポートの通信制限をしていない場合はこちらの項を実施する必要がございません。

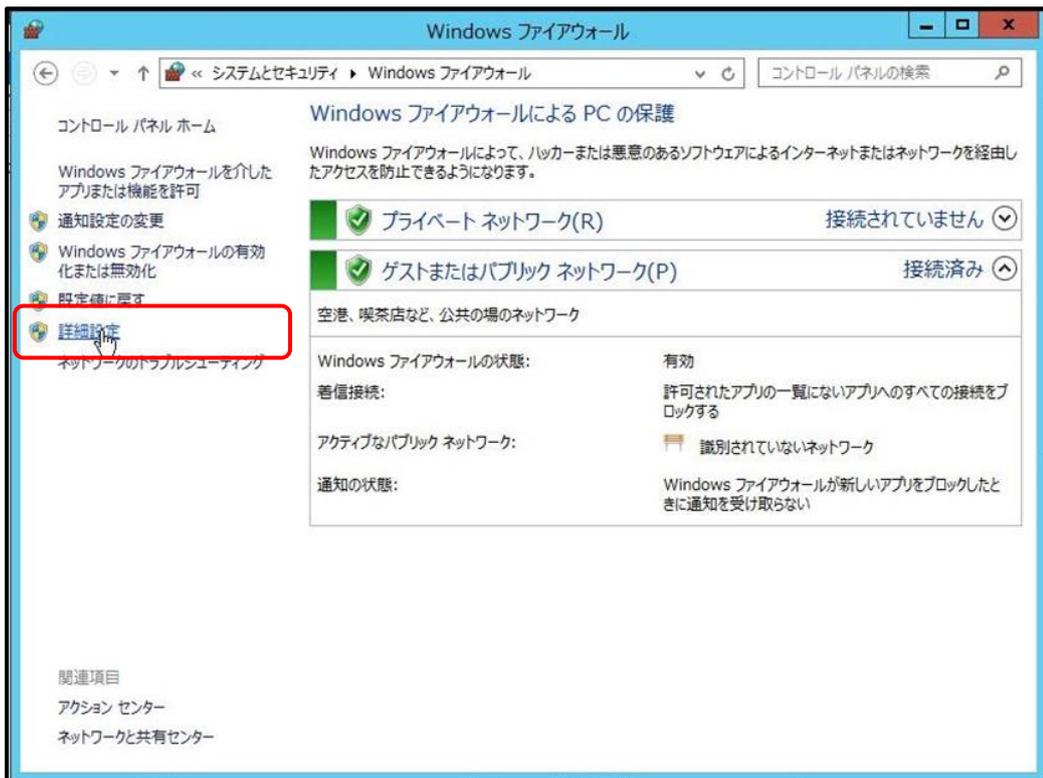
Zabbix 監視ではポート「10050」を利用しております。

Windows ファイアウォールでポートを利用許可する設定をご案内します。

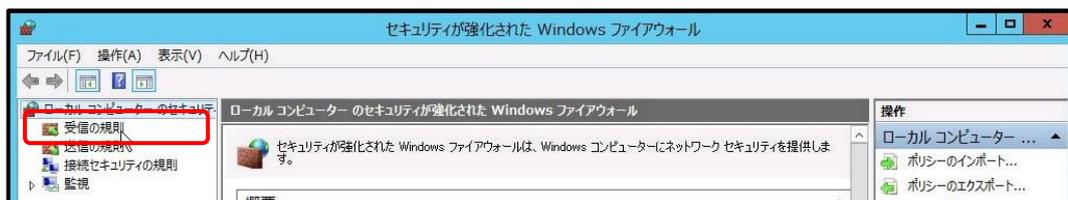
- ① コントロールパネルから「システムとセキュリティ」→「Windows ファイアウォール」を選択します。



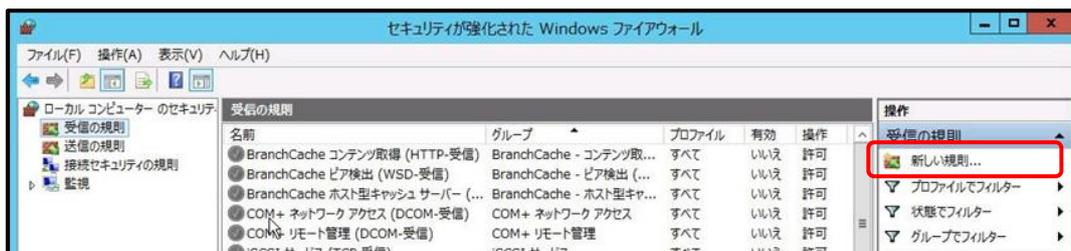
- ② Windows ファイアウォールの設定画面から「詳細設定」を選択します。



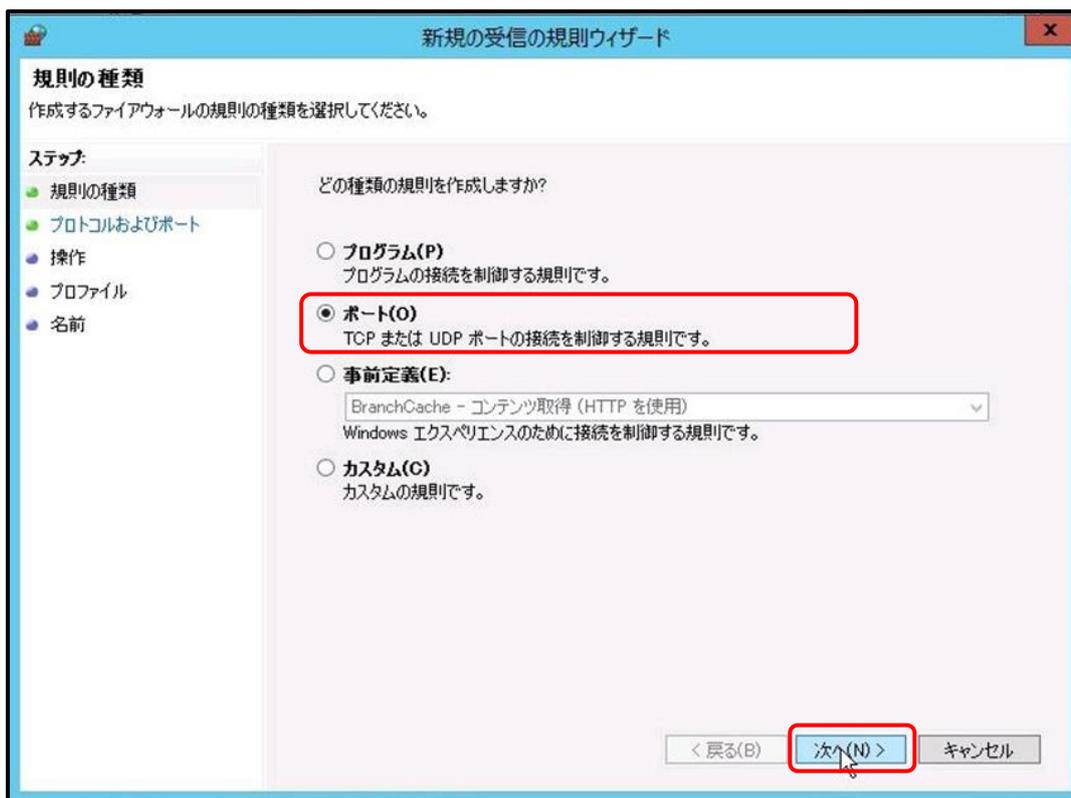
- ③ 詳細設定画面から「受信の規則」を選択します。



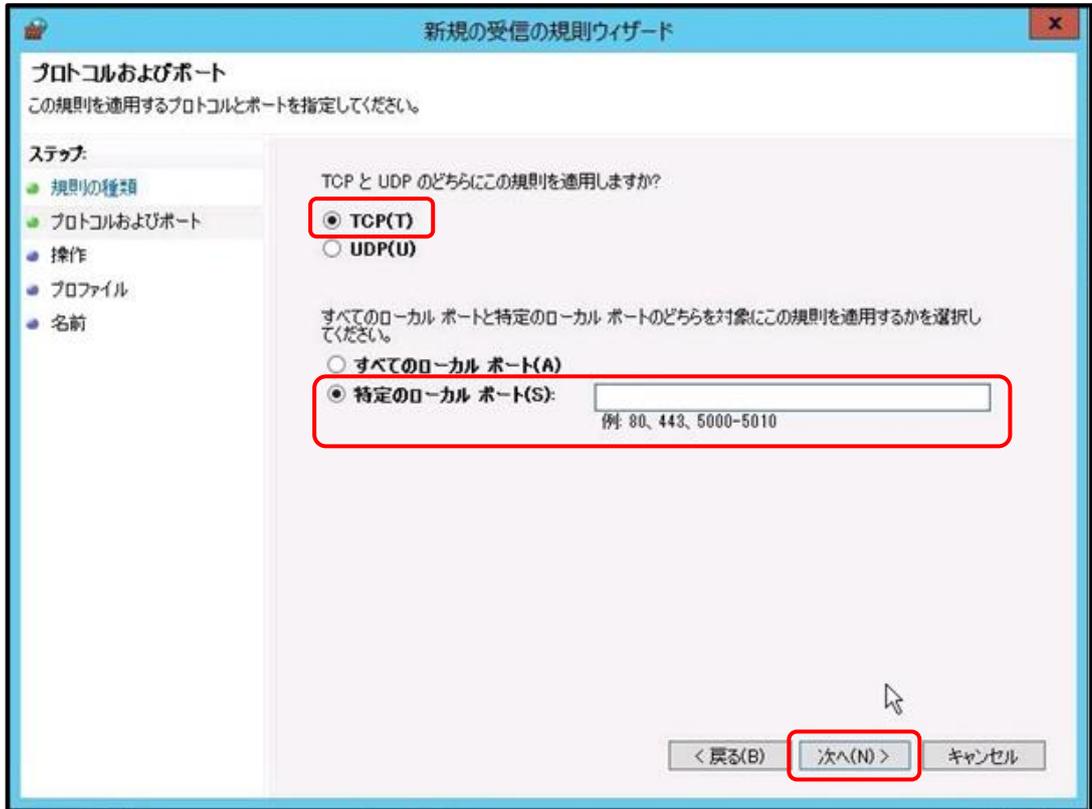
- ④ 画面右側のペインから、「新しい規則」を選択します。



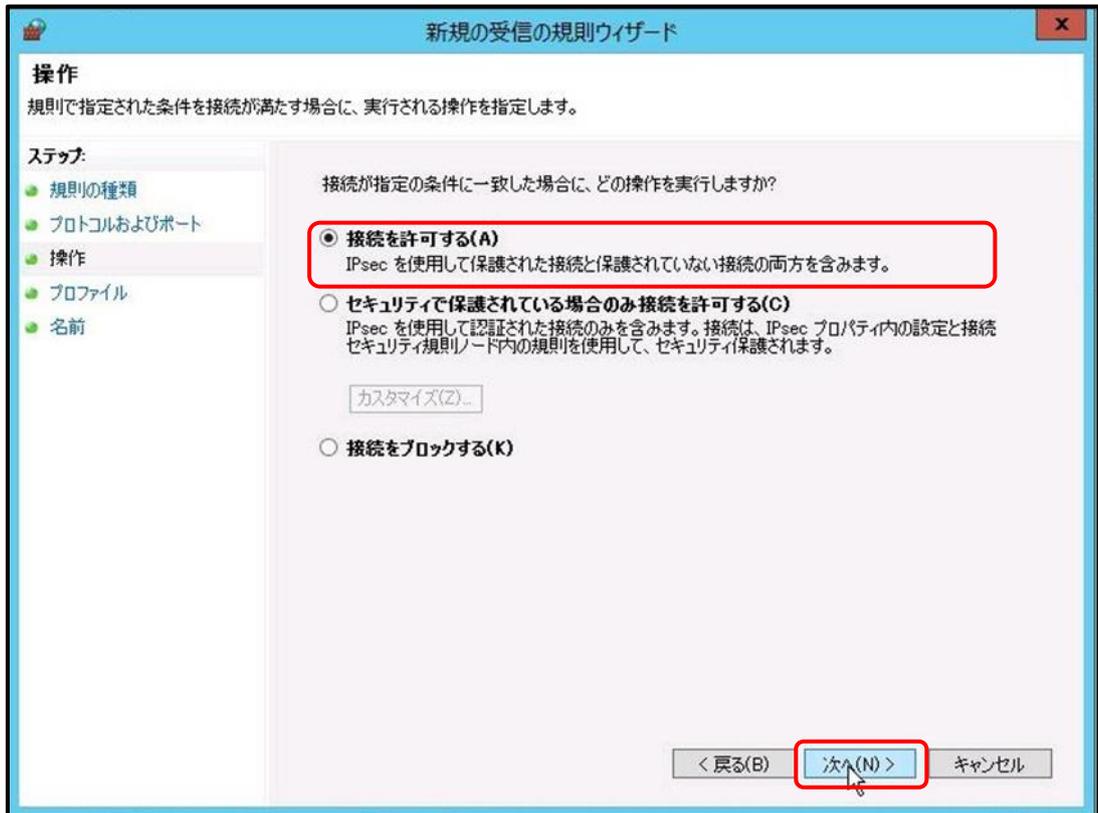
- ⑤ 作成するファイアウォール規則の選択で「ポート」を選択して「次へ」を押下します。



- ⑥ プロトコルおよびポートの設定で以下の内容を入力して「次へ」を押下します。
 TCP/UDP の選択 : ラジオボタンにて「TCP」を選択します
 ローカルポート : ラジオボタンにて「特定のローカルポート(S)」を選択して、
 : 入力欄にポート番号「10050」を入力します。



- ⑦ 指定した接続に対する操作として「接続を許可する」を選択して「次へ」を押下します。



- ⑧ 適用するプロファイルの選択はデフォルト(全てチェック)のまま「次へ」を押下します。

The screenshot shows the '新規の受信の規則ウィザード' (New Inbound Rule Wizard) dialog box. The title bar is blue with a close button (X) on the right. The main window has a light blue header with the title. Below the header, the text reads 'プロフィール' (Profile) and 'この規則が適用されるプロフィールを指定してください。' (Specify the profile to which this rule will be applied). On the left, there is a 'ステップ' (Steps) sidebar with five items: '規則の種類' (Rule Type), 'プロトコルおよびポート' (Protocol and Port), '操作' (Action), 'プロフィール' (Profile), and '名前' (Name). The 'プロフィール' step is currently selected. The main area contains the question 'この規則はいつ適用しますか?' (When should this rule be applied?). Below this, there are three checked options: 'ドメイン(D)' (Domain) with the description 'コンピューターがその企業ドメインに接続しているときに適用されます。' (Applied when the computer is connected to its corporate domain.); 'プライベート(P)' (Private) with 'コンピューターが自宅や職場などのプライベート ネットワークに接続しているときに適用されます。' (Applied when the computer is connected to a private network like home or office.); and 'パブリック(U)' (Public) with 'コンピューターがパブリック ネットワークに接続しているときに適用されます。' (Applied when the computer is connected to a public network.). At the bottom right, there are three buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel). The '次へ(N) >' button is highlighted with a red box.

- ⑨ 規則の名前として「Zabbix_Agent」を入力して「完了」を押下します。

The screenshot shows the '新規の受信の規則ウィザード' (New Inbound Rule Wizard) dialog box. The title bar is blue with a close button (X) on the right. The main window has a light blue header with the title. Below the header, the text reads '名前' (Name) and 'この規則の名前と説明を指定してください。' (Specify the name and description of this rule). On the left, there is a 'ステップ' (Steps) sidebar with five items: '規則の種類' (Rule Type), 'プロトコルおよびポート' (Protocol and Port), '操作' (Action), 'プロフィール' (Profile), and '名前' (Name). The '名前' step is currently selected. The main area contains two input fields: '名前(N):' (Name) and '説明 (オプション)(O):' (Description (Optional)). The '名前(N):' field is highlighted with a red box. At the bottom right, there are three buttons: '< 戻る(B)' (Back), '完了(F)' (Finish), and 'キャンセル' (Cancel). The '完了(F)' button is highlighted with a red box.

2.5 スタティックルート（静的経路）追加設定

弊社の監視サービスは「ローカルネットワーク」を経由し「監視サーバー」と「監視対象 VM」が通信を行います。そのためスタティックルートの設定が必要となります。

事前に設定完了通知に記載されているローカルネットワークをご確認ください。

- ① コマンドプロンプトにて、下記コマンドを実行し、スタティックルートの設定をします。

```
> route add 192.168.251.241 mask 255.255.255.0 ローカル NW のゲートウェイ IP
```

```
例) route add 192.168.251.241 mask 255.255.255.0 10.1.4.254
```

- ② 恒久的な設定をするためには、オプションで `-p` を指定します。

```
> route add -p 192.168.251.241 mask 255.255.255.0 ローカル NW のゲートウェイ IP
```

```
例) route add -p 192.168.251.241 mask 255.255.255.0 10.1.4.254
```

- ③ ルーティングテーブルを表示して、経路が追加されている事を確認します。

```
> route print -4 *251.241
```

出力例)

```
IPv4 ルート テーブル
```

```
=====
```

```
アクティブ ルート:
```

ネットワーク宛先	ネットマスク	ゲートウェイ	インターフェイス	メトリック
192.168.251.241	255.255.255.0	リンク上	10.0.1.2	276

- ④ Zabbix サーバーへ ping を実施し疎通を確認します。

```
> ping 192.168.251.241
```

Zabbix-Agent のインストール及び設定は以上です。

3 VMware vCloud Director からの CD マウント

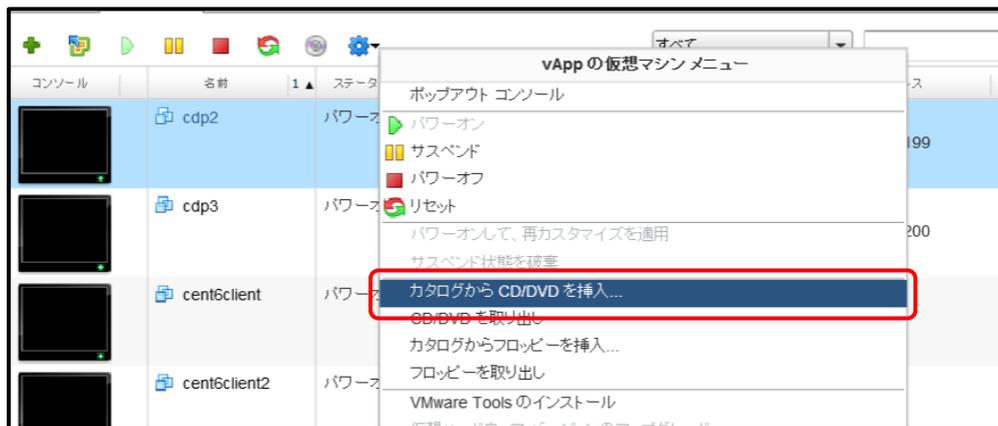
本項では、VMware vCloud Director (以降 vCD) 環境において、仮想マシンに CD/DVD メディアをマウント/アンマウントするための操作をご案内しております。

あらかじめ WEB ブラウザから vCD の Web 管理画面にログインした上で以下の手順を実施します。

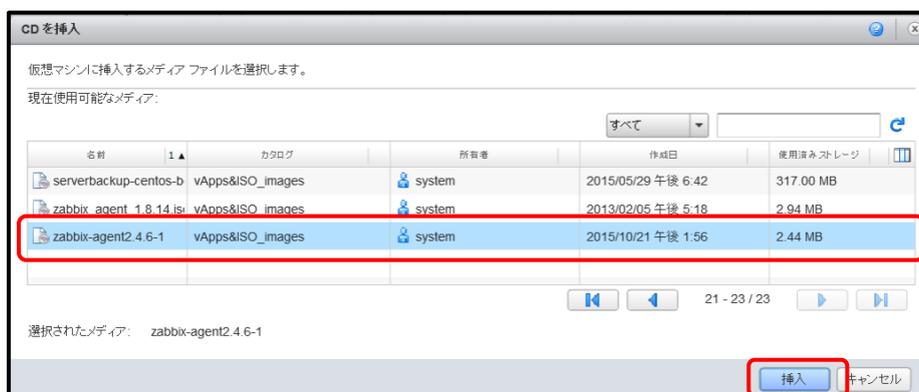
3.1 仮想サーバーへのメディアの挿入

弊社からエージェントのパッケージが含まれた ISO イメージを公開しておりますので、公開カタログよりインストールメディアを選択して仮想サーバーに挿入します。

- ① 「マイクラウド」 → 「vApp」 → 「仮想マシン」 から任意の仮想マシンを選択して、右クリックから「カタログから CD/DVD を挿入」を実行します。



- ② メディアの選択画面に遷移しますので「zabbix-agent3.0.7-8」の iso イメージを選択の上、画面下部の「挿入」ボタンを押下します。



3.2 仮想サーバーでのマウント／アンマウント操作

3.2.1 Windows サーバーでのマウント操作

Windows サーバーでは vCD からのメディアの挿入操作後、OS が自動認識で CD/DVD メディアをマウントします。

3.2.2 Windows サーバーでのアンマウント操作

Windows サーバーでのメディアの取り出しは、DVD ドライブを右クリックして「取り出し」を実行します。

3.2.3 Linux サーバーでのマウント操作

- ① マウント用のディレクトリを作成します

```
# mkdir /mnt/cdrom
```

- ② メディアのマウントを実施します

```
# mount /dev/cdrom /mnt/cdrom
```

3.2.4 Linux サーバーでのアンマウント操作

- ① メディアのアンマウントを実施します。

パッケージをインストール後にアンマウントを必ず実施します。

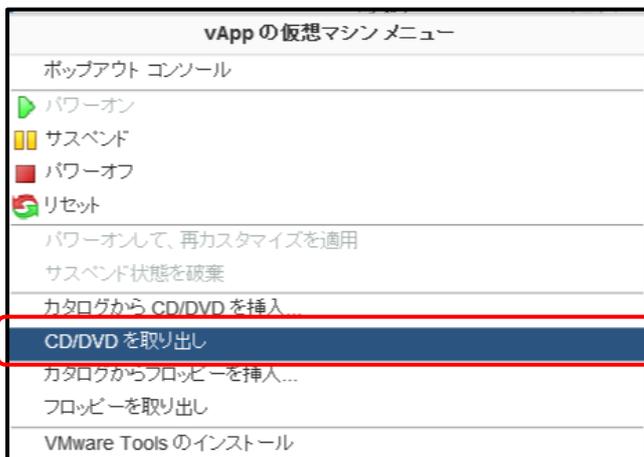
```
# umount /mnt/cdrom
```

- ② マウント用のディレクトリを削除します

```
# rmdir /mnt/cdrom
```

3.3 仮想サーバーからのメディアの取り出し

挿入時と同じように vCD の WEB 管理画面から対象の仮想マシンを右クリックし「CD/DVD の取り出し」を実施します。



※必ず事前に仮想サーバー上でメディアのアンマウント操作を実行下さい。

以上