

AWS上での監視サーバー(Zabbix)構築【6.監視登録(ICMPノード監視)】

AWS



AWS上での監視サーバー(Zabbix)構築【6.監視登録(ICMPノード監視)】

2021.09.12 2021.09.11

監視サーバーをAWS上で構築し、CML上のネットワーク機器/サーバーを監視します。監視ソフトウェアはZabbixを利用します。

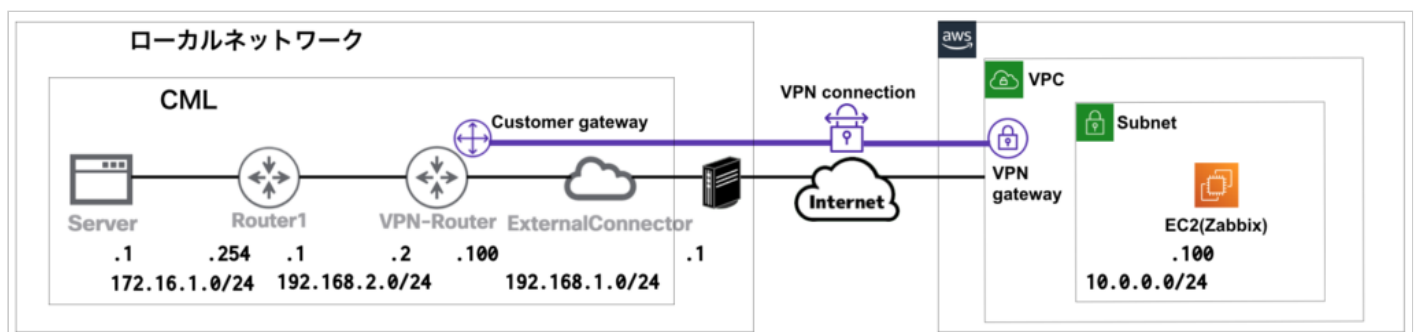
[【前回】AWS上での監視サーバー\(Zabbix\)構築【5.AWSとCMLのVPN接続】](#)

[【次回】AWS上での監視サーバー\(Zabbix\)構築【7.監視登録\(SNMP\)】](#)

ネットワーク構成

下記のネットワーク環境を構築し、AWS上のEC2(Zabbixサーバー)から、CML上のネットワーク機器/サーバーを監視できるようにしていきます。

[【参考】AWSサイト間VPNの構築（1.AWSの基本設定）](#)

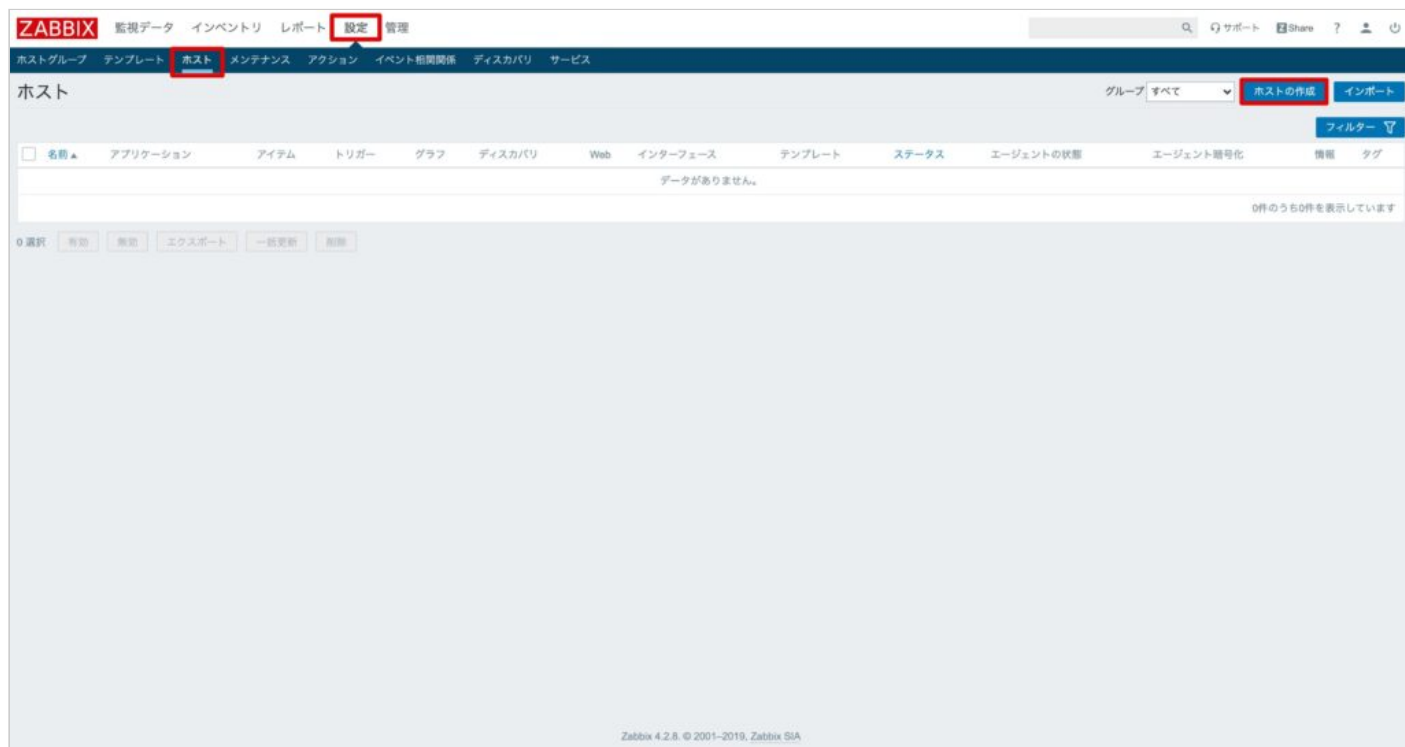


Zabbixの監視登録（ICMPノード監視）

Pingによるノード監視(死活監視)ができるように監視登録を行います。

ホストの作成

「設定」→「ホスト」を選択し、「ホストの作成」をクリックします。



Serverを設定します。“ホスト名”と“表示名”は任意の名前を設定します。Zabbixでは、ホストは少なくとも一つのグループに所属する必要があるため、“CML-001”というグループを新規設定しています。

ZABBIX 監視データ インベントリ レポート 設定 管理

ホストグループ テンプレート ホスト メンテナンス アクション イベント相関関係 ディスカバリ サービス

ホスト

ホスト テンプレート IPMI タグ マクロ インベントリ 暗号化

* ホスト名 Server

表示名 Server

* グループ CML-001| 選択
CML-001 (新規)

エージェントのインターフェース

IPアドレス	DNS名	接続方法	ポート	標準
127.0.0.1		IPアドレス DNS	10050	<input checked="" type="radio"/> 削除
追加				

SNMPインターフェース [追加](#)

JMXインターフェース [追加](#)

IPMIインターフェース [追加](#)

説明

プロキシによる監視 (プロキシなし) ▼

有効 ☒

[追加](#) [キャンセル](#)

“エージェントのインターフェース”にServerのIPアドレスを設定します。

ZABBIX 監視データ インベントリ レポート 設定 管理

ホストグループ テンプレート ホスト メンテナンス アクション イベント相関関係 ディスカバリ サービス

ホスト

ホスト テンプレート IPMI タグ マクロ インベントリ 暗号化

* ホスト名

Server

表示名

Server

* グループ

CML-001 (新規) ✕

検索文字列を入力

選択

* 少なくとも1つ以上のインターフェースが存在する必要があります。

エージェントのインターフェース	IPアドレス	DNS名	接続方法	ポート	標準
	172.16.1.1		IPアドレス	DNS	10050

追加

削除

SNMPインターフェース

追加

JMXインターフェース

追加

IPMIインターフェース

追加

説明

プロキシによる監視 (プロキシなし) ▼

有効 ☒

追加 キャンセル

Zabbixの標準で用意されているICMP監視のテンプレートを適用します。

「テンプレート」を選択し、「新規テンプレートをリンク」の右の「選択」をクリックします。

ZABBIX 監視データ インベントリ レポート 設定 管理

ホストグループ テンプレート ホスト メンテナンス アクション イベント相関関係 ディスカバリ サービス

ホスト

ホスト テンプレート IPMI タグ マクロ インベントリ 暗号化

テンプレートとのリンク

名前

アクション

新規テンプレートをリンク

検索文字列を入力

選択

追加

追加 キャンセル

テンプレートの一覧が表示されるので、「Template Module ICMP Ping」にチェックを入れ、「選択」をクリックします。

テンプレート

グループ Templates

☐ Template Module Cisco CISCO-MEMORY-POOL-MIB SNMPv2

☐ Template Module Cisco CISCO-PROCESS-MIB IOS versions 12.0_3_T-12.2_3.5 SNMPv2

☐ Template Module Cisco CISCO-PROCESS-MIB SNMPv2

☐ Template Module Cisco Inventory SNMPv2

☐ Template Module Cisco OLD-CISCO-CPU-MIB SNMPv2

☐ Template Module EtherLike-MIB SNMPv1

☐ Template Module EtherLike-MIB SNMPv2

☐ Template Module Generic SNMPv1

☐ Template Module Generic SNMPv2

☐ Template Module HOST-RESOURCES-MIB SNMPv1

☐ Template Module HOST-RESOURCES-MIB SNMPv2

☒ Template Module ICMP Ping

☐ Template Module Interfaces Simple SNMPv1

☐ Template Module Interfaces Simple SNMPv2

☐ Template Module Interfaces SNMPv1

☐ Template Module Interfaces SNMPv2

☐ Template Module Interfaces Windows SNMPv2

☐ Template Net Alcatel Timetra TiMOS SNMPv2

☐ Template Net Arista SNMPv2

☐ Template Net Brocade FC SNMPv2

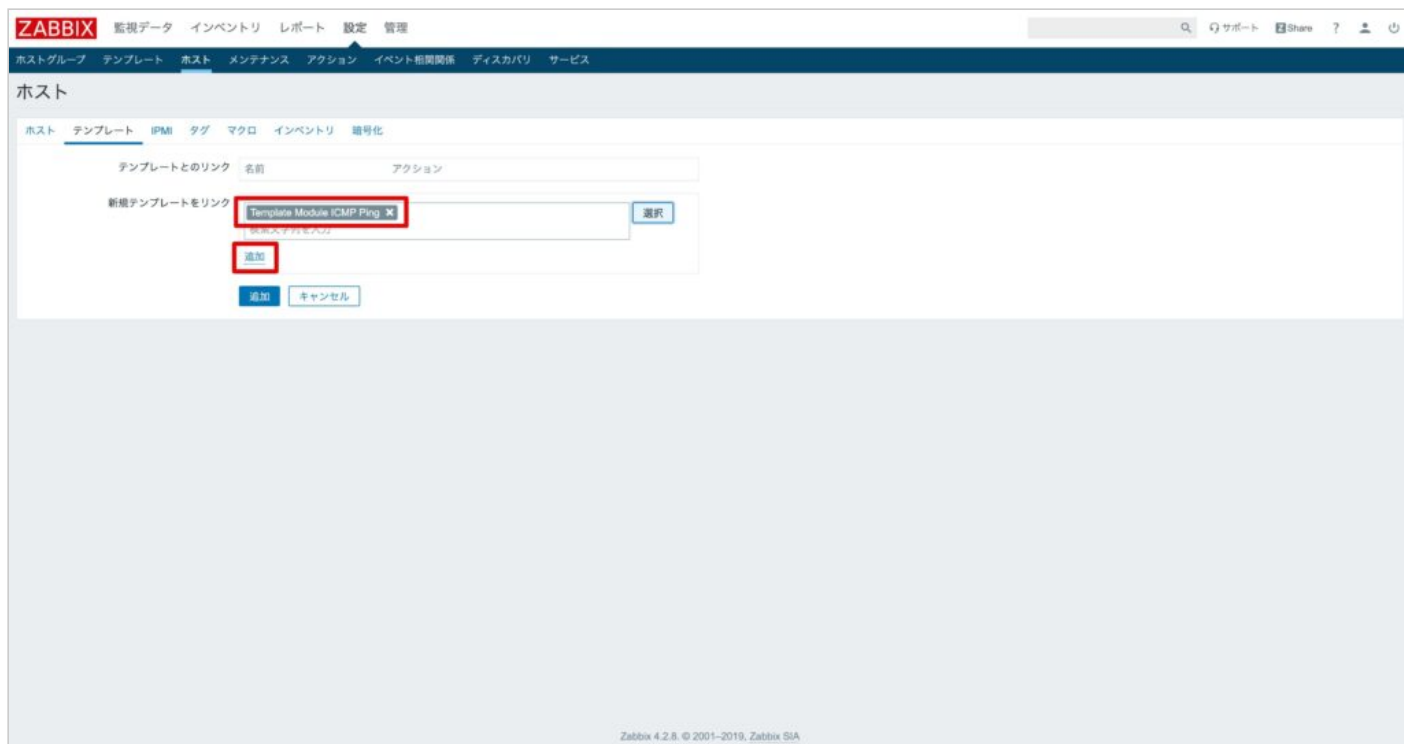
☐ Template Net Brocade_Foundry Nonstackable SNMPv2

☐ Template Net Brocade_Foundry Stackable SNMPv2

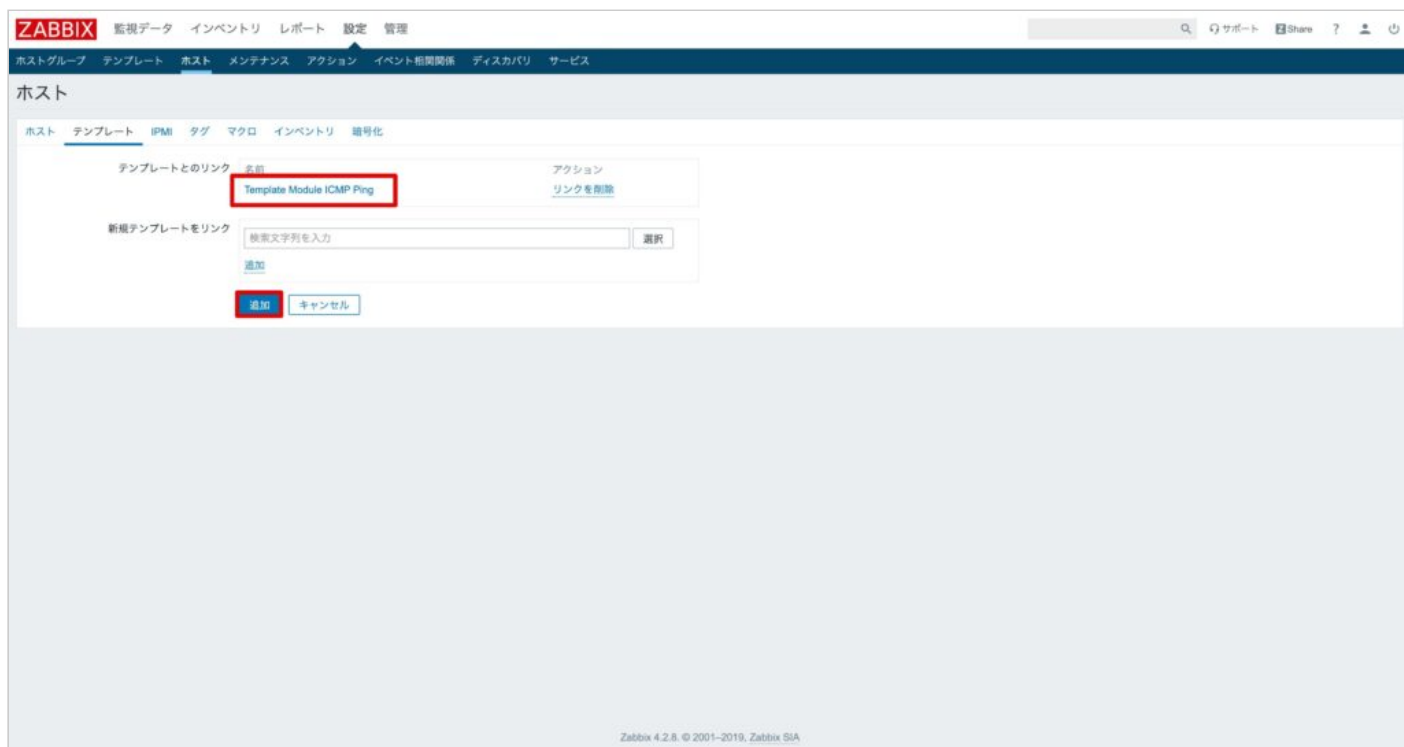
選択

キャンセル

“新規テンプレートをリンク”に選択したテンプレートが表示されていることを確認し、「追加」をクリックします。



“テンプレートとのリンク”に追加されたことを確認し、「追加」をクリックします。



ホストが追加されていることを確認します。※表示されない場合は、右上の「グループ」で作成したグループを選択してください。

The screenshot shows the Zabbix 4.2.8 web interface. The 'Hosts' tab is active, and the 'CML-001' group is selected. A red box highlights the 'Server' host in the table. Below the table, there are buttons for '0 選択', '有効', '無効', 'エクスポート', '一括更新', and '削除'.

名前	アプリケーション	アイテム	トリガー	グラフ	ディスカバリ	Web	インターフェース	テンプレート	ステータス	エージェントの状態	エージェント番号	情報	タグ
Server	アプリケーション 1	アイテム 3	トリガー 3	グラフ	ディスカバリ	Web	172.16.1.1: 10050	Template Module ICMP Ping	有効	ZBX SNMP JMX IPMI	なし		

同様に、「VPN-Router」と「Router1」も追加します。

The screenshot shows the Zabbix 4.2.8 web interface with three hosts listed: 'Router1', 'Server', and 'VPN-Router'. A red box highlights all three hosts in the table. Below the table, there are buttons for '0 選択', '有効', '無効', 'エクスポート', '一括更新', and '削除'.

名前	アプリケーション	アイテム	トリガー	グラフ	ディスカバリ	Web	インターフェース	テンプレート	ステータス	エージェントの状態	エージェント番号	情報	タグ
Router1	アプリケーション 1	アイテム 3	トリガー 3	グラフ	ディスカバリ	Web	192.168.2.1: 10050	Template Module ICMP Ping	有効	ZBX SNMP JMX IPMI	なし		
Server	アプリケーション 1	アイテム 3	トリガー 3	グラフ	ディスカバリ	Web	172.16.1.1: 10050	Template Module ICMP Ping	有効	ZBX SNMP JMX IPMI	なし		
VPN-Router	アプリケーション 1	アイテム 3	トリガー 3	グラフ	ディスカバリ	Web	192.168.1.100: 10050	Template Module ICMP Ping	有効	ZBX SNMP JMX IPMI	なし		

障害検知確認

Router1のGi0/1をリンクダウンさせて、ServerにPingが通らないようにします。

```
[Router1]
int Gi0/1
shut
```

「監視データ」→「障害」の画面で、Serverの障害として検知されていることを確認します。※デフォルト設定では、1分毎のPingが3回連続でタイムアウトすると障害として検知します。そのため、障害発生から検知までの時間は3分～4分程度かかります。

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害	継続時間	確認済	アクション	タグ
06:06:07	重症の障害		障害		Server	Unavailable by ICMP ping	1m 5s	いいえ		

Router1のGi0/1をリンクアップさせて、障害を復旧します。

```
[Router1]
int Gi0/1
no shut
```

Serverの障害が復旧していることを確認します。(ステータスが解決済みとなります。)*復旧時は次のPingが成功した時点で、復旧として扱われます。そのため、1分以内に復旧が検知されます。

時間	深刻度	復旧時刻	ステータス	情報	ホスト	障害	継続時間	確認済	アクション	タグ
06:06:07	重症の障害	06:08:07	解決済		Server	Unavailable by ICMP ping	2m	いいえ		

パケットキャプチャ確認

ZabbixからのICMP通信をCML上でキャプチャして確認します。

1分毎に3回ずつPingを実施していることがわかります。赤枠内が障害発生中で、ServerからPing応答がない時間帯です。

No.	Time	Source	Destination	Protocol	Length	Info
1	06:49:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57c8, seq=0/0, ttl=253 (reply in 2)
2	06:49:07	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57c8, seq=0/0, ttl=63 (request in 1)
3	06:49:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57c8, seq=1/256, ttl=253 (reply in 4)
4	06:49:08	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57c8, seq=1/256, ttl=63 (request in 3)
5	06:49:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57c8, seq=2/512, ttl=253 (reply in 6)
6	06:49:09	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57c8, seq=2/512, ttl=63 (request in 5)
7	06:50:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57dc, seq=0/0, ttl=253 (reply in 8)
8	06:50:07	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57dc, seq=0/0, ttl=63 (request in 7)
9	06:50:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57dc, seq=1/256, ttl=253 (reply in 10)
10	06:50:08	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57dc, seq=1/256, ttl=63 (request in 9)
11	06:50:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57dc, seq=2/512, ttl=253 (reply in 12)
12	06:50:09	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x57dc, seq=2/512, ttl=63 (request in 11)
13	06:51:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57ea, seq=0/0, ttl=253 (no response found!)
14	06:51:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57ea, seq=1/256, ttl=253 (no response found!)
15	06:51:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57ea, seq=2/512, ttl=253 (no response found!)
16	06:52:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57f9, seq=0/0, ttl=253 (no response found!)
17	06:52:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57f9, seq=1/256, ttl=253 (no response found!)
18	06:52:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x57f9, seq=2/512, ttl=253 (no response found!)
19	06:53:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5807, seq=0/0, ttl=253 (no response found!)
20	06:53:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5807, seq=1/256, ttl=253 (no response found!)
21	06:53:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5807, seq=2/512, ttl=253 (no response found!)
22	06:54:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5815, seq=0/0, ttl=253 (no response found!)
23	06:54:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5815, seq=1/256, ttl=253 (no response found!)
24	06:54:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5815, seq=2/512, ttl=253 (no response found!)
25	06:55:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5847, seq=0/0, ttl=253 (reply in 26)
26	06:55:07	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5847, seq=0/0, ttl=63 (request in 25)
27	06:55:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5847, seq=1/256, ttl=253 (reply in 28)
28	06:55:08	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5847, seq=1/256, ttl=63 (request in 27)
29	06:55:09	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5847, seq=2/512, ttl=253 (reply in 30)
30	06:55:09	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5847, seq=2/512, ttl=63 (request in 29)
31	06:56:07	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5855, seq=0/0, ttl=253 (reply in 32)
32	06:56:07	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5855, seq=0/0, ttl=63 (request in 31)
33	06:56:08	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5855, seq=1/256, ttl=253 (reply in 34)
34	06:56:08	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5855, seq=1/256, ttl=63 (request in 33)
35	06:56:10	10.0.0.100	172.16.1.1	ICMP	98	Echo (ping) request id=0x5855, seq=2/512, ttl=253 (reply in 36)
36	06:56:10	172.16.1.1	10.0.0.100	ICMP	98	Echo (ping) reply id=0x5855, seq=2/512, ttl=63 (request in 35)

以上で、AWS上での監視サーバー(Zabbix)構築【6.監視登録(ICMPノード監視)】の説明は完了です！