

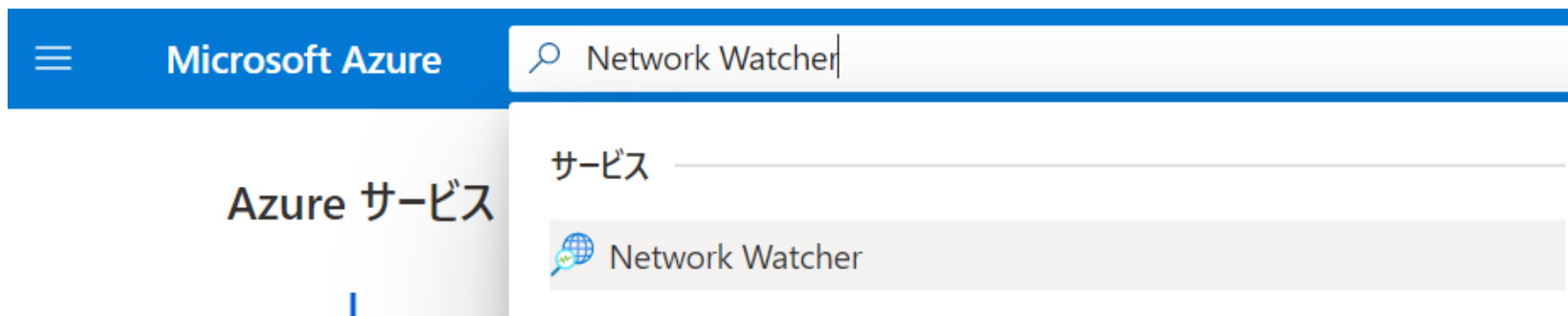
Network Watcher

Azure Network Watcher は、Azure 仮想ネットワーク内のリソースの監視、診断、メトリックの表示、ログの有効化または無効化を行うツールを提供します。

PaaS 監視または Web 分析を対象としたものではなく、それらには使用できません。

Network Watcherは
VNetの監視と診断に
利用できる

App Serviceの監視には、
「Application Insights」
「Azure Monitor」 「Log
Analytics」を利用でき
る。



<https://docs.microsoft.com/ja-jp/azure/azure-monitor/>

<https://docs.microsoft.com/ja-jp/azure/architecture/reference-architectures/app-service-web-app/app-monitoring>

監視

トポロジ

接続モニター

接続モニター (プレビュー)

ネットワーク パフォーマンス モニター

ネットワーク診断ツール

IP フローの確認

次ホップ

有効なセキュリティ ルール

VPN のトラブルシューティング

パケット キャプチャ

接続のトラブルシューティング

メトリック

使用量 + クォータ

ログ

NSG フロー ログ

診断ログ

トラフィック分析

ダウンロード トポロジ

SVGでダウンロード

サブスクリプション ⓘ

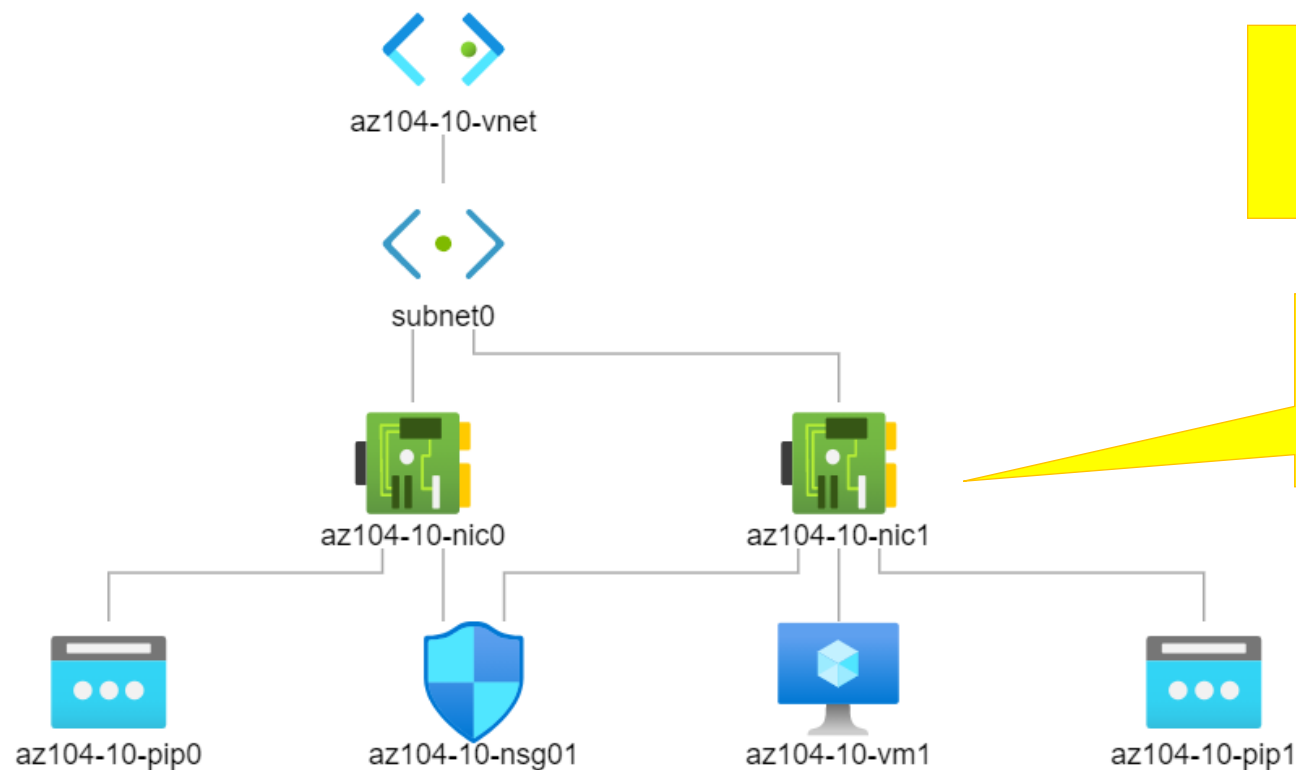
Azure Pass - スポンサー プラン 2020-1...

リソース グループ ⓘ

az104-10-rg0

Virtual Network ⓘ

az104-10-vnet



選択したVNetが
図で表示される

クリックで
リソースの
画面へ移動

マウスホイールで
拡大縮小

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

接続モニターの追加



名前 *

monitor1



ソース

サブスクリプション *



Azure Pass - スポンサー プラン 2020-10-26



仮想マシン *

az104-10-vm1



宛先



仮想マシンの選択



手動で指定

URI、FQDN または IPv4 *

https://portal.azure.com/



ポート *



443



^ 詳細設定

発信元ポート

プローブ間隔 (秒)

既定値: 60

追加

接続モニターを作成しています...


接続モニターを作成


接続元VMを選択


接続先のVMやアドレスを入力


デフォルトでは
60秒ごとに
プローブ (探査)

監視


 トポロジ


 接続モニター


 接続モニター (プレビュー)

 ネットワーク パフォーマンス モニター


ネットワーク診断ツール


 IP フローの確認

 次ホップ

 有効なセキュリティ ルール

 VPN のトラブルシューティング

 パケット キャプチャ


 接続のトラブルシューティング


メトリック

 使用量 + クォータ

ログ

 NSG フロー ログ

 診断ログ

 トラフィック分析

+ 追加

Network Watcher 接続モニターを使用することで、接続の到達可能性、待機時間、ネットワークトポロジの変更を構成および追跡することができます。問題がある場合に、発生した原因とその修正方法が示されます。[詳細。](#)

名前 ①	サブスクリプション ①	リソース グループ ①	仮想マシン ①
名前でフィルター	Azure Pass - スポンサー プラン 2020-10-26	すべてのリソース グループ	すべての仮想マシン

名前	リソース グループ	ソース	ポート	宛先	ポート	状態	間隔 (秒)	
monitor1	az104-10-rg0	az104-10-vm1	-	portal.azure.com	443	Running	60	...

追加した
接続モニターが
一覧に表示される

使わない場合は
停止しておくことも
可能

間隔 (秒)

削除

停止

開始

監視

トポロジ

接続モニター

接続モニター (プレビュー)

ネットワーク パフォーマンス モニター

ネットワーク診断ツール

IP フローの確認

次ホップ

有効なセキュリティ ルール

VPN のトラブルシューティング

パケット キャプチャ

接続のトラブルシューティング

メトリック

使用量 + クォータ

ログ

NSG フロー ログ

診断ログ

トラフィック分析

名前	リソース グループ	ソース	ポート	宛先	ポート	状態	間隔 (秒)	
monitor1	az104-10-rg0	az104-10-vm1	-	portal.azure.com	443	Running	60	...



状態

✓ 到達可能

エージェントの拡張機能のバージョン

1.4

ソース 仮想マシン

az104-10-vm1

次に指定する直近の期間のデータを表示する:

1 時間

6 時間

12 時間

1 日間

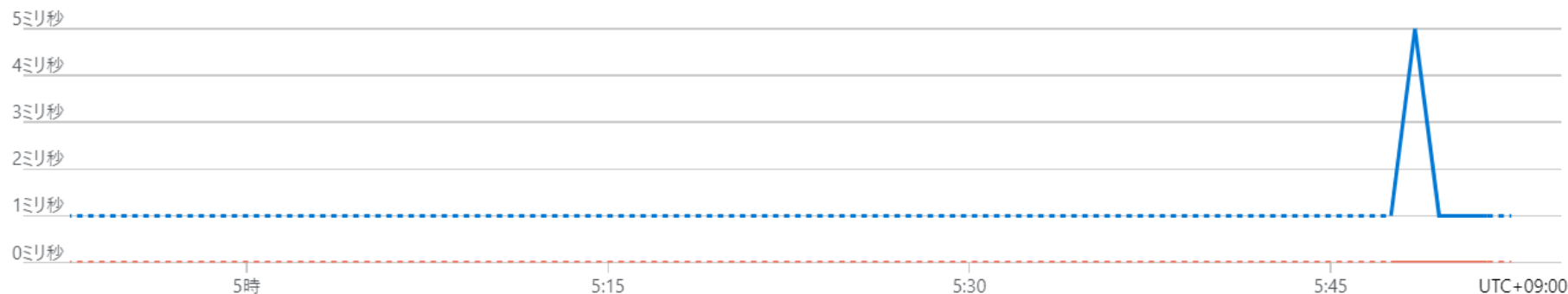
7 日

30 日

到達可能性 (connection reachability)

平均往復時間と % プロブが失敗しました

平均往復時間 (RTT) と、
失敗したプロブの割合 (% Probes Failed)



Avg. Round-trip Time...
networkwatcher_eastu...

1.8ミリ秒

% Probes Failed (平均)
networkwatcher_eastu...

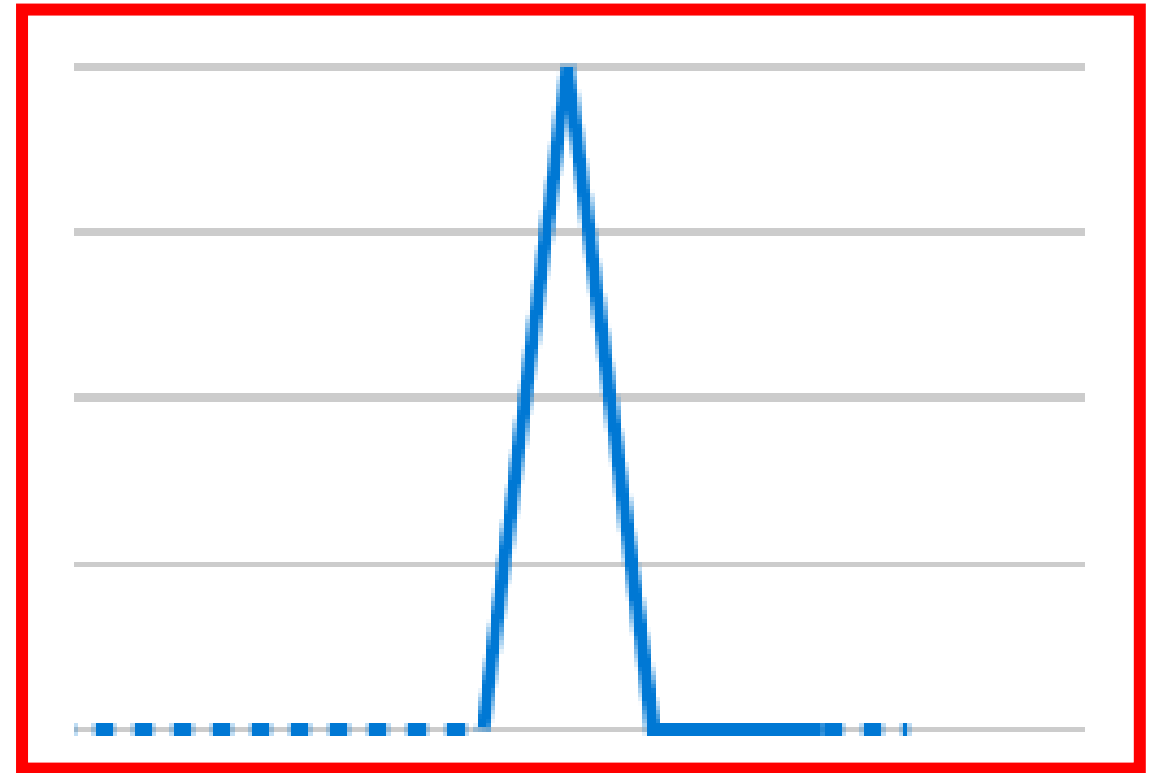
0%

Avg. Round-trip Time...
networkwatcher_eastu...

1.8 ミリ秒

% Probes Failed (平均)
networkwatcher_eastu...

0 %



5:45

UTC+09:00

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

★NPMとは？

+ NPM の追加



Network Watcher から Network Performance Monitor にアクセスできるようになりました。これにより、ネットワーク監視の要件を一元的に表示できます。Network Performance Monitor (NPM) を使用してハイブリッド接続を監視するには、NPM に関連付けられているワークスペースがサポート対象リージョンにあることをご確認ください。サポート対象リージョンの一覧は[ここ](#)で確認できます。

サブスクリプション ⓘ

Azure Pass - スポンサー プラン 2020-10-26



ワークスペース名で検索します

ワークスペース名

場所

loganalytics1234234

japaneast

Network Performance Monitorの
Log Analytics ワークスペースへ接続

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

仮想マシン * ⓘ

az104-10-vm1

VM

ネットワーク インターフェイス *

az104-10-nic1

パケットの詳細

プロトコル

☒ TCP ☐ UDP

プロトコル

方向

☐ 受信 ☒ 送信

通信方向

ローカル IP アドレス * ⓘ

10.0.0.4

ローカル ポート * ⓘ

55555

ローカル (VM) のポート

リモート IP アドレス * ⓘ

8.8.8.8

リモート ポート * ⓘ

53

リモートのIPとポート

チェック



アクセス許可

許可 (拒否) の判定結果

セキュリティ規則

AllowInternetOutBound

どのセキュリティ規則で許可 (拒否) されたか

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

仮想マシン * ⓘ

az104-10-vm1

VM

ネットワーク インターフェイス *

az104-10-nic1

ソース IP アドレス * ⓘ

10.0.0.4

接続先 IP アドレス * ⓘ

8.8.8.8

接続先IP

次ホップ

結果

次ホップの種類

Internet

IP アドレス

-

ルート テーブル ID

System Route



次ホップの種類

どのルートテーブルを
使用したか

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

仮想マシン *

az104-10-vm1

VM

以下のネットワーク インターフェイスを 1 つ選んで、それに関連付けられている有効なセキュリティ ルールとネットワーク セキュリティ グループを表示します。

スコープ

仮想マシン (az104-10-vm1)

ネットワーク インターフェイス

az104-10-nic1

NIC

関連付けられた NSG: ①

nsg-nic (ネットワーク インターフェイス), nsg-subnet (サブネット)



プレフィックスの拡張されたリストを表示するには、規則行をクリックします。

NICやサブネットに関連付けられた
NSGを選択

nsg-nic

nsg-subnet

受信規則

名前	↑↓	優先度	↑↓	ソース	発信元ポート	↑↓	宛先	宛先ポート	↑↓	プロトコル	↑↓	アク
Port_3389		100		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	3389-3389		TCP		✓
AllowVnetInBound		65000		仮想ネットワーク (2 プレフィックス)	0-65535		仮想ネットワーク (2 プレフィックス)	0-65535		すべて		✓
AllowAzureLoadBalancerInBound		65001		Azure Load Balancer (2 プレフィッ...	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		すべて		✓
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		すべて		✗

送信規則

名前	↑↓	優先度	↑↓	ソース	発信元ポート	↑↓	宛先	宛先ポート	↑↓	プロトコル	↑↓	アク
AllowVnetOutBound		65000		仮想ネットワーク (2 プレフィックス)	0-65535		仮想ネットワーク (2 プレフィックス)	0-65535		すべて		✓
AllowInternetOutBound		65001		0.0.0.0/0,0.0.0.0/0	0-65535		インターネット (201 プレフィックス)	0-65535		すべて		✓
DenyAllOutBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		すべて		✗

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

nsg-nic

nsg-subnet

受信規則

名前	↑↓	優先度	↑↓	ソース	発信元ポート	↑↓	宛先
Port_3389		100		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0
AllowVnetInBound		65000		仮想ネットワーク (2 プレフィックス)	0-65535		仮想ネットワーク (2 プレフィックス)
AllowAzureLoadBalancerInBound		65001		Azure Load Balancer (2 プレフィッ...	0-65535		0.0.0.0/0,0.0.0.0/0
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0

アドレスのプレフィックス

AllowVnetInBound

ソース 宛先

10.0.0.0/24

168.63.129.16/32

ルールの行をクリックすると、
アドレスのプレフィックス
(ソース/宛先) を
確認できる

(参考) VM > 設定 > ネットワーク にも、同様の画面がある

az104-10-vm1 | ネットワーク

仮想マシン

検索 (Ctrl+/)

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

設定

ネットワーク

接続

ディスク

サイズ

セキュリティ

Advisor の推奨事項

拡張機能

継続的デリバリー

可用性とスケールリング

構成

ID

プロパティ

ロック

操作

Bastion

自動シャットダウン

ネットワーク インターフェイスの接続

ネットワーク インターフェイスのデタッチ

az104-10-nic1

IP 構成 ⓘ

ipconfig1 (プライマリ)

ネットワーク インターフェイス: az104-10-nic1

有効なセキュリティ ルール

トポロジ

仮想ネットワーク/サブネット: az104-10-vnet/subnet0

NIC パブリック IP: 104.45.159.229

NIC プライベート IP: 10.0.0.4

高速ネットワーク: 無効

受信ポートの規則

送信ポートの規則

アプリケーションのセキュリティ グループ

負荷分散

ネットワーク セキュリティ グループ nsg-subnet (サブネットに接続: subnet0)

影響 1 サブネット、0 ネットワーク インターフェイス

受信ポートの規則を追加する

優先度	名前	ポート	プロトコル	ソース	宛先
100	Port_80	80	TCP	任意	任意
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNet
65001	AllowAzureLoadBalancerIn...	任意	任意	AzureLoadBalancer	任意
65500	DenyAllInBound	任意	任意	任意	任意

ネットワーク セキュリティ グループ nsg-nic (ネットワーク インターフェイスに接続: az104-10-nic1)

影響 0 サブネット、1 ネットワーク インターフェイス

受信ポートの規則を追加する

優先度	名前	ポート	プロトコル	ソース	宛先
100	Port_3389	3389	TCP	任意	任意
65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNet
65001	AllowAzureLoadBalancerIn...	任意	任意	AzureLoadBalancer	任意
65500	DenyAllInBound	任意	任意	任意	任意

各VMの設定の確認、
ルールの追加・変更は
こちらが便利

サブネットの
NSG

NICの
NSG

監視



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

- VPNゲートウェイまたは接続の正常性を診断
- 診断が完了すると、結果（Healthy / UnHealthy）、
- エラーの原因（「事前共有キーが一致していない」等）を表示

▶ Start troubleshooting

Choose a subscription

Resource group

Location

* Storage account

[Click here to select storage container](#)



	NAME	TROUBLESHOOTING STATUS	RESOURCE STATUS	RESOURCE GROUP	LOCATION
<input type="checkbox"/>	▼ DemoVnet1Gw	Not started	Succeeded	PortalTestRg	West Central US
<input type="checkbox"/>	Vnet1toVnet2Connection	Not started	Failed	PortalTestRg	West Central US
<input type="checkbox"/>	Vnet2toVnet1Connection	Not started	Succeeded	PortalTestRg	West Central US
<input type="checkbox"/>	▼ DemoVnet2Gw	Not started	Succeeded	PortalTestRg	West Central US
<input type="checkbox"/>	Vnet1toVnet2Connection	Not started	Failed	PortalTestRg	West Central US
<input type="checkbox"/>	Vnet2toVnet1Connection	Not started	Succeeded	PortalTestRg	West Central US

Details

Status

Action

Resource

DemoVnet1Gw



トポロジ



接続モニター



接続モニター (プレビュー)



ネットワーク パフォーマンス モニター

ネットワーク診断ツール



IP フローの確認



次ホップ



有効なセキュリティ ルール



VPN のトラブルシューティング



パケット キャプチャ



接続のトラブルシューティング

メトリック



使用量 + クォータ

ログ



NSG フロー ログ



診断ログ



トラフィック分析

パケット キャプチャを追加する



サブスクリプション *

Azure Pass - スポンサー プラン 2020-10-26

リソース グループ *

az104-10-rg0

ターゲット仮想マシン *

az104-10-vm1

パケット キャプチャ名 *

packetcapture1

構成のキャプチャ

パケット キャプチャ出力ファイル (.cap) は、ストレージ アカウントおよび/またはターゲット VM に格納できます。

☒ ストレージ アカウント ☐ ファイル ☐ 両方

ストレージ アカウント *

cs110032000f1062fbe

1 パケットあたりの最大バイト数 ⓘ

既定値: 0 (パケット全体)

1 セッションあたりの最大バイト数 ⓘ

既定値: 1073741824

制限時間 (秒) ⓘ

既定値: 18000

保存

キャンセル

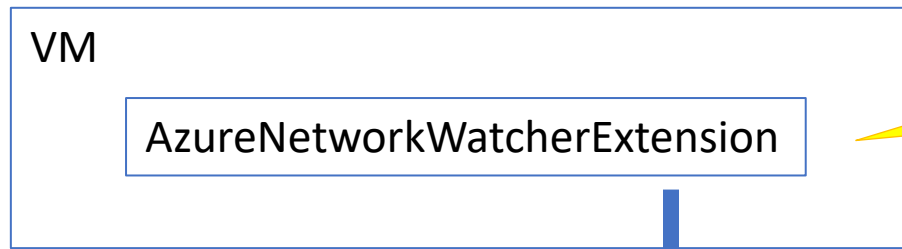
VM

任意のキャプチャ名

キャプチャ出力ファイルの保存先

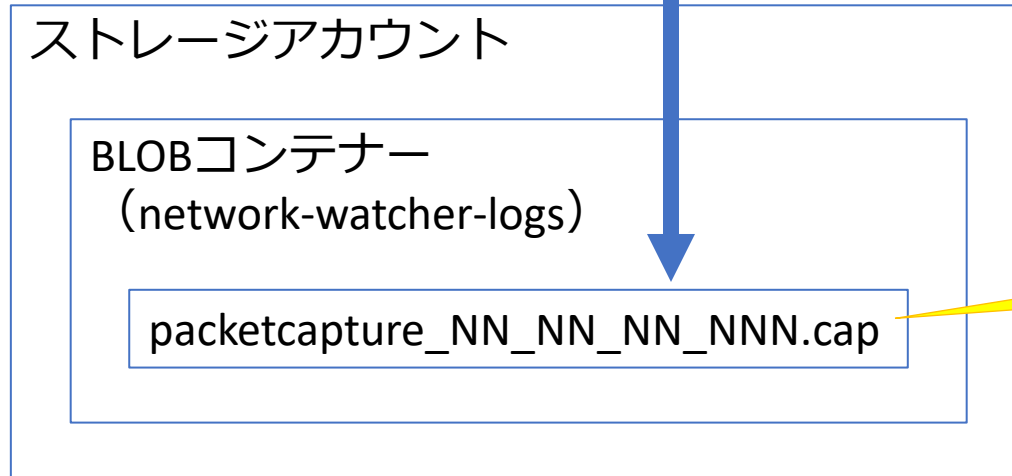
出力先の
ストレージ アカウント

制限時間など



パケット キャプチャ
拡張機能

追記



追加BLOBとして保存される

network-watcher-logs / subscriptions / a1e4fbf9-7099-4568-960e-1c7f6e7308c1 / resourcegroups / az104-10-rg0 / providers / microsoft.compute / virtualmachines / az104-10-vm1 / 2020 / 10 / 28 / **packetcapture_NN_NN_NN.cap**

監視

- トポロジ
- 接続モニター
- 接続モニター (プレビュー)
- ネットワーク パフォーマンス モニター

ネットワーク診断ツール

- IP フローの確認
- 次ホップ
- 有効なセキュリティ ルール
- VPN のトラブルシューティング
- パケット キャプチャ
- 接続のトラブルシューティング


メトリック

- 使用量 + クォータ

ログ

- NSG フロー ログ
- 診断ログ
- トラフィック分析













名前	リソースの種類	リソース グループ	状態	場所
az104-10-nsg01	ネットワーク セキュリティ グ...	az104-10-rg0	⊖ 無効	米国東部
nsg-nic	ネットワーク セキュリティ グ...	az104-10-rg0	⊖ 無効	米国東部
nsg-subnet	ネットワーク セキュリティ グ...	az104-10-rg0	⊖ 無効	米国東部



Azure Pass - スポンサー プラン 2020-10-26 | リソース プロバイダー

サブスクリプション

設定

-  プログラムによるデプロイ
-  リソース グループ
-  リソース
-  プレビュー機能
-  使用量 + クォータ
-  ポリシー
-  管理証明書
-  アクセス許可
-  **リソース プロバイダー**
-  デプロイ
-  プロパティ
-  リソースのロック

 登録

 登録解除

 更新

 insights 

プロバイダー	状態
Microsoft.OperationallInsights	Registered
Microsoft.D365CustomerInsights	NotRegistered
microsoft.insights	NotRegistered
Microsoft.PolicyInsights	NotRegistered
Microsoft.SecurityInsights	NotRegistered
Microsoft.TimeSeriesInsights	NotRegistered

ネットワーク診断ツール

メトリック

ログ

フロー ログ設定

保存 破棄

フロー ログ

ストレージ アカウントにデータを送信すると、ストレージとトランザクションに対する通常データ レートを請求されます。

状態

オフ

オン

フロー ログのバージョン ⓘ

バージョン 1

バージョン 2

バージョン 1 では、許可トラフィックと拒否トラフィックの両方について、イングレスおよびエグレス IP トラフィック フローが記録されます。バージョン 2 では、フローごとのその他のスループット情報 (バイト数とパケット数) を提供します。
[詳細](#)。

ストレージ アカウント

storage92837492734

リテンション期間 (日数) ⓘ




1

フロー ログを保存する
ストレージアカウント
を選択

※NSGと同じリージョンの
ストレージアカウント

0日にすると
永続的に保存

 構成済みのストレージ アカウントからフロー ログをダウンロードできました。

名前	リソースの種類	リソース グループ	状態	場所
 az104-10-nsg01	ネットワーク セキュリティ グ...	az104-10-rg0	 有効	米国東部
 nsg-nic	ネットワーク セキュリティ グ...	az104-10-rg0	 有効	米国東部
 nsg-subnet	ネットワーク セキュリティ グ...	az104-10-rg0	 有効	米国東部



insights-logs-networksecuritygroupflowevent

コンテナー

検索 (Ctrl+/)



アップロード



アクセス レベルを変更します



更新



削除

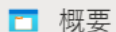


層の変更



リースの取得

...



概要



アクセス制御 (IAM)

設定



アクセス ポリシー



プロパティ



メタデータ

認証方法: アクセス キー (Azure AD のユーザー アカウントに切り替える)

場所: insights-logs-networksecuritygroupflowevent / resourceId= / SUBSCRIPTIONS / A1E4FBF9-7099-4568-960E-1C7F6E7308C1 / RESOURCEGROUPS / AZ104-10-RG0 / PROVIDERS / MICROSOFT.NETWORK / NETWORKSECURITYGROUPS / NSG-NIC / y=2020 / m=10 / d=28 / h=23 / m=00 / macAddress=000D3A9E90AD

プレフィックスによる BLOB の検索 (大文字と小文字を区別)



削除された Blob を表示

名前

変更日時

アクセス層

BLOB の種類



[...]



PT1H.json

2020/10/29 8:36:51

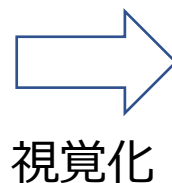
ホット (推定)

ブロック BLOB

NSG フロー ログの活用

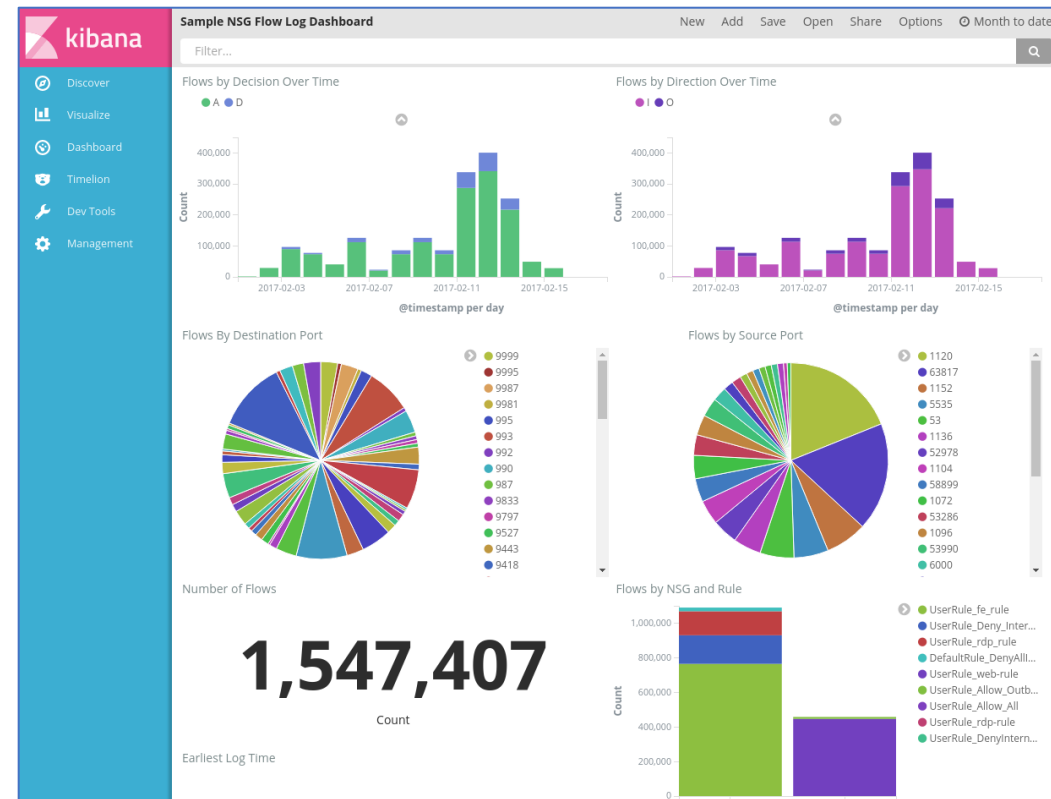
NSGフロー ログ ファイル (JSON)

```
{
  "records": [
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_AllowInternetOutBound",
      "flow": {
        "direction": "Outbound",
        "protocol": "TCP",
        "sourceIp": "1603927970",
        "sourcePort": "10.0.0.4",
        "destinationIp": "20.42.6.197",
        "destinationPort": "59956",
        "bytes": "443",
        "packets": "T",
        "action": "Allow"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_DenyAllInBound",
      "flow": {
        "direction": "Inbound",
        "protocol": "TCP",
        "sourceIp": "1603927967",
        "sourcePort": "45.129.33.24",
        "destinationIp": "10.0.0.4",
        "destinationPort": "46078",
        "bytes": "2096",
        "packets": "T",
        "action": "Deny"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_AllowInternetOutBound",
      "flow": {
        "direction": "Outbound",
        "protocol": "TCP",
        "sourceIp": "1603927971",
        "sourcePort": "125",
        "destinationIp": "10.0.0.4",
        "destinationPort": "37822",
        "bytes": "8088",
        "packets": "T",
        "action": "Allow"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_DenyAllInBound",
      "flow": {
        "direction": "Inbound",
        "protocol": "TCP",
        "sourceIp": "1603927991",
        "sourcePort": "96.127.158.235",
        "destinationIp": "10.0.0.4",
        "destinationPort": "65116",
        "bytes": "3389",
        "packets": "T",
        "action": "Deny"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_AllowInternetOutBound",
      "flow": {
        "direction": "Outbound",
        "protocol": "TCP",
        "sourceIp": "1603927967",
        "sourcePort": "185",
        "destinationIp": "10.0.0.4",
        "destinationPort": "53254",
        "bytes": "3389",
        "packets": "T",
        "action": "Allow"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_DenyAllInBound",
      "flow": {
        "direction": "Inbound",
        "protocol": "TCP",
        "sourceIp": "1603927974",
        "sourcePort": "185.193.88.12",
        "destinationIp": "10.0.0.4",
        "destinationPort": "53254",
        "bytes": "3389",
        "packets": "T",
        "action": "Deny"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_AllowInternetOutBound",
      "flow": {
        "direction": "Outbound",
        "protocol": "TCP",
        "sourceIp": "1603927978",
        "sourcePort": "188.126.89.194",
        "destinationIp": "10.0.0.4",
        "destinationPort": "45556",
        "bytes": "3389",
        "packets": "T",
        "action": "Allow"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_DenyAllInBound",
      "flow": {
        "direction": "Inbound",
        "protocol": "TCP",
        "sourceIp": "1603927994",
        "sourcePort": "45.146.164.72",
        "destinationIp": "10.0.0.4",
        "destinationPort": "57266",
        "bytes": "3389",
        "packets": "T",
        "action": "Deny"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_AllowInternetOutBound",
      "flow": {
        "direction": "Outbound",
        "protocol": "TCP",
        "sourceIp": "1603928009",
        "sourcePort": "185.193.88.12",
        "destinationIp": "10.0.0.4",
        "destinationPort": "49760",
        "bytes": "3389",
        "packets": "T",
        "action": "Allow"
      }
    },
    {
      "time": "2020-10-28T23:33:40.024078",
      "category": "NetworkSecurityGroupFlowEvent",
      "resourceId": "PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/...",
      "rule": "DefaultRule_DenyAllInBound",
      "flow": {
        "direction": "Inbound",
        "protocol": "TCP",
        "sourceIp": "1603928009",
        "sourcePort": "185.193.88.12",
        "destinationIp": "10.0.0.4",
        "destinationPort": "49760",
        "bytes": "3389",
        "packets": "T",
        "action": "Deny"
      }
    }
  ]
}
```



視覚化

Kibana や Power BI で分析



ルールごとの送信および受信フロー、フローが適用されている NIC、フローに関する 5 組の情報 (送信元/送信先 IP、送信元/送信先ポート、プロトコル)、およびトラフィックの許可/拒否の状況