Troubleshoot a hybrid VPN connection

10/08/2018 • 8 minutes to read • Contributors

In this article

This article gives some tips for troubleshooting a VPN gateway connection between an on-premises network and Azure. For general information on troubleshooting common VPN-related errors, see Troubleshooting common VPN related errors.

Verify the VPN appliance is functioning correctly

The following recommendations are useful for determining if your on-premises VPN appliance is functioning correctly.

Check any log files generated by the VPN appliance for errors or failures. This will help you determine if the VPN appliance is functioning correctly. The location of this information will vary according to your appliance. For example, if you are using RRAS on Windows Server 2012, you can use the following PowerShell command to display error event information for the RRAS service:

```
Get-EventLog -LogName System -EntryType Error -Source RemoteAccess | Format-List -Property *
```

The *Message* property of each entry provides a description of the error. Some common examples are:

- Inability to connect, possibly due to an incorrect IP address specified for the Azure VPN gateway in the RRAS VPN network interface configuration.

```
EventID            : 20111
MachineName        : on-premises-vm
Data               : {41, 3, 0, 0}
Index              : 14231
Category           : (0)
CategoryNumber     : 0
EntryType          : Error
Message            : RoutingDomainID- {00000000-0000-0000-0000-000000000000}: A demand dial
connection to the remote
                        interface AzureGateway on port VPN2-4 was successfully initiated
but failed to complete
                        successfully because of the  following error: The network connec-
tion between your computer and
                        the VPN server could not be established because the remote server
is not responding. This could
                        be because one of the network devices (for example, firewalls, NAT,
routers, and so on) between your computer
                        and the remote server is not configured to allow VPN connections.
Please contact your
                        Administrator or your service provider to determine which device
may be causing the problem.
Source             : RemoteAccess
ReplacementStrings : {{00000000-0000-0000-0000-000000000000}, AzureGateway, VPN2-4, The
network connection between
                        your computer and the VPN server could not be established because
the remote server is not
                        responding. This could be because one of the network devices (for
example, firewalls, NAT, routers, and so on)
                        between your computer and the remote server is not configured to
allow VPN connections. Please
                        contact your Administrator or your service provider to determine
which device may be causing the
                        problem.}
InstanceId         : 20111
TimeGenerated      : 3/18/2016 1:26:02 PM
TimeWritten        : 3/18/2016 1:26:02 PM
UserName           :
Site               :
Container          :
```

- The wrong shared key being specified in the RRAS VPN network interface configuration.

```
EventID            : 20111
MachineName        : on-premises-vm
Data               : {233, 53, 0, 0}
Index              : 14245
Category           : (0)
CategoryNumber     : 0
EntryType          : Error
Message            : RoutingDomainID- {00000000-0000-0000-0000-000000000000}: A demand dial
connection to the remote
                        interface AzureGateway on port VPN2-4 was successfully initiated
but failed to complete
                        successfully because of the  following error: Internet key exchange
(IKE) authentication credentials are unacceptable.

Source             : RemoteAccess
ReplacementStrings : {{00000000-0000-0000-0000-000000000000}, AzureGateway, VPN2-4, IKE au-
thentication credentials are
                        unacceptable.
                        }
InstanceId         : 20111
TimeGenerated      : 3/18/2016 1:34:22 PM
TimeWritten        : 3/18/2016 1:34:22 PM
UserName           :
Site               :
Container          :
```

You can also obtain event log information about attempts to connect through the RRAS service using the following PowerShell command:

```
Get-EventLog -LogName Application -Source RasClient | Format-List -Property *
```

In the event of a failure to connect, this log will contain errors that look similar to the following:

```
EventID            : 20227
MachineName        : on-premises-vm
Data               : {}
Index              : 4203
Category           : (0)
CategoryNumber     : 0
EntryType          : Error
```

```
Message            : CoId={B4000371-A67F-452F-AA4C-3125AA9CFC78}: The user SYSTEM dialed a con-
nection named
                        AzureGateway that has failed. The error code returned on failure is
809.
Source             : RasClient
ReplacementStrings : {{B4000371-A67F-452F-AA4C-3125AA9CFC78}, SYSTEM, AzureGateway, 809}
InstanceId         : 20227
TimeGenerated      : 3/18/2016 1:29:21 PM
TimeWritten        : 3/18/2016 1:29:21 PM
UserName           :
Site               :
Container          :
```

Verify connectivity

Verify connectivity and routing across the VPN gateway. The VPN appliance may not be correctly routing traffic through the Azure VPN Gateway. Use a tool such as PsPing to verify connectivity and routing across the VPN gateway. For example, to test connectivity from an on-premises machine to a web server located on the VNet, run the following command (replacing `<<web-server-address>>` with the address of the web server):

```
PsPing -t <<web-server-address>>:80
```

If the on-premises machine can route traffic to the web server, you should see output similar to the following:

```
D:\PSTools>psping -t 10.20.0.5:80

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 10.20.0.5:80:
Infinite iterations (warmup 1) connecting test:
Connecting to 10.20.0.5:80 (warmup): 6.21ms
Connecting to 10.20.0.5:80: 3.79ms
Connecting to 10.20.0.5:80: 3.44ms
Connecting to 10.20.0.5:80: 4.81ms

    Sent = 3, Received = 3, Lost = 0 (0% loss),
    Minimum = 3.44ms, Maximum = 4.81ms, Average = 4.01ms
```

If the on-premises machine cannot communicate with the specified destination, you will see messages like this:

```
D:\PSTools>psping -t 10.20.1.6:80

PsPing v2.01 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to 10.20.1.6:80:
Infinite iterations (warmup 1) connecting test:
Connecting to 10.20.1.6:80 (warmup): This operation returned because the timeout period ex-
pired.
Connecting to 10.20.1.6:80: This operation returned because the timeout period expired.
Connecting to 10.20.1.6:80: This operation returned because the timeout period expired.
Connecting to 10.20.1.6:80: This operation returned because the timeout period expired.
Connecting to 10.20.1.6:80:
    Sent = 3, Received = 0, Lost = 3 (100% loss),
    Minimum = 0.00ms, Maximum = 0.00ms, Average = 0.00ms
```

Verify that the on-premises firewall allows VPN traffic to pass and that the correct ports are opened.

Verify that the on-premises VPN appliance uses an encryption method that is compatible with the Azure VPN gateway. For policy-based routing, the Azure VPN gateway supports the AES256, AES128, and 3DES encryption algorithms. Route-based gateways support AES256 and 3DES. For more information, see About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections.

Check for problems with the Azure VPN gateway

The following recommendations are useful for determining if there is a problem with the Azure VPN gateway:

Examine Azure VPN gateway diagnostic logs for potential issues. See Step-by-Step: Capturing Azure Resource Manager VNET Gateway Diagnostic Logs.

Verify that the Azure VPN gateway and on-premises VPN appliance are configured with the same shared authentication key. You can view the shared key stored by the Azure VPN gateway using the following Azure CLI command:

```
azure network vpn-connection shared-key show <<resource-group>> <<vpn-connection-name>>
```

Use the command appropriate for your on-premises VPN appliance to show the shared key configured for that appliance.

Verify that the *GatewaySubnet* subnet holding the Azure VPN gateway is not associated with an NSG.

You can view the subnet details using the following Azure CLI command:

```
azure network vnet subnet show -g <<resource-group>> -e <<vnet-name>> -n GatewaySubnet
```

Ensure there is no data field named *Network Security Group ID*. The following example shows the results for an instance of the *GatewaySubnet* that has an assigned NSG (*VPN-Gateway-Group*). This can prevent the gateway from working correctly if there are any rules defined for this NSG.

```
C:\>azure network vnet subnet show -g profx-prod-rg -e profx-vnet -n GatewaySubnet
    info:    Executing command network vnet subnet show
    + Looking up virtual network "profx-vnet"
    + Looking up the subnet "GatewaySubnet"
    data:    Id                              : /subscriptions/########-####-####-####-
############/resourceGroups/profx-prod-rg/providers/Microsoft.Network/virtualNetworks/profx-
vnet/subnets/GatewaySubnet
    data:    Name                            : GatewaySubnet
    data:    Provisioning state              : Succeeded
    data:    Address prefix                  : 10.20.3.0/27
    data:    Network Security Group id       : /subscriptions/########-####-####-####-
############/resourceGroups/profx-prod-
rg/providers/Microsoft.Network/networkSecurityGroups/VPN-Gateway-Group
    info:    network vnet subnet show command OK
```

Verify that the virtual machines in the Azure VNet are configured to permit traffic coming in from outside the VNet. Check any NSG rules associated with subnets containing these virtual machines. You can view all NSG rules using the following Azure CLI command:

```
azure network nsg show -g <<resource-group>> -n <<nsg-name>>
```

Verify that the Azure VPN gateway is connected. You can use the following Azure PowerShell command to check the current status of the Azure VPN connection. The `<<connection-name>>` parameter is the name of the Azure VPN connection that links the virtual network gateway and the local gateway.

```
Get-AzureRmVirtualNetworkGatewayConnection -Name <<connection-name>> - ResourceGroupName <<re-
source-group>>
```

The following snippets highlight the output generated if the gateway is connected (the first example), and disconnected (the second example):

```
PS C:\> Get-AzureRmVirtualNetworkGatewayConnection -Name profx-gateway-connection -Resource-
GroupName profx-prod-rg

AuthorizationKey           :
VirtualNetworkGateway1     : Microsoft.Azure.Commands.Network.Models.PSVirtualNetworkGateway
VirtualNetworkGateway2     :
LocalNetworkGateway2       : Microsoft.Azure.Commands.Network.Models.PSLocalNetworkGateway
Peer                       :
ConnectionType             : IPsec
RoutingWeight              : 0
SharedKey                  : ####################################
ConnectionStatus           : Connected
EgressBytesTransferred     : 55254803
IngressBytesTransferred    : 32227221
ProvisioningState          : Succeeded
...
```

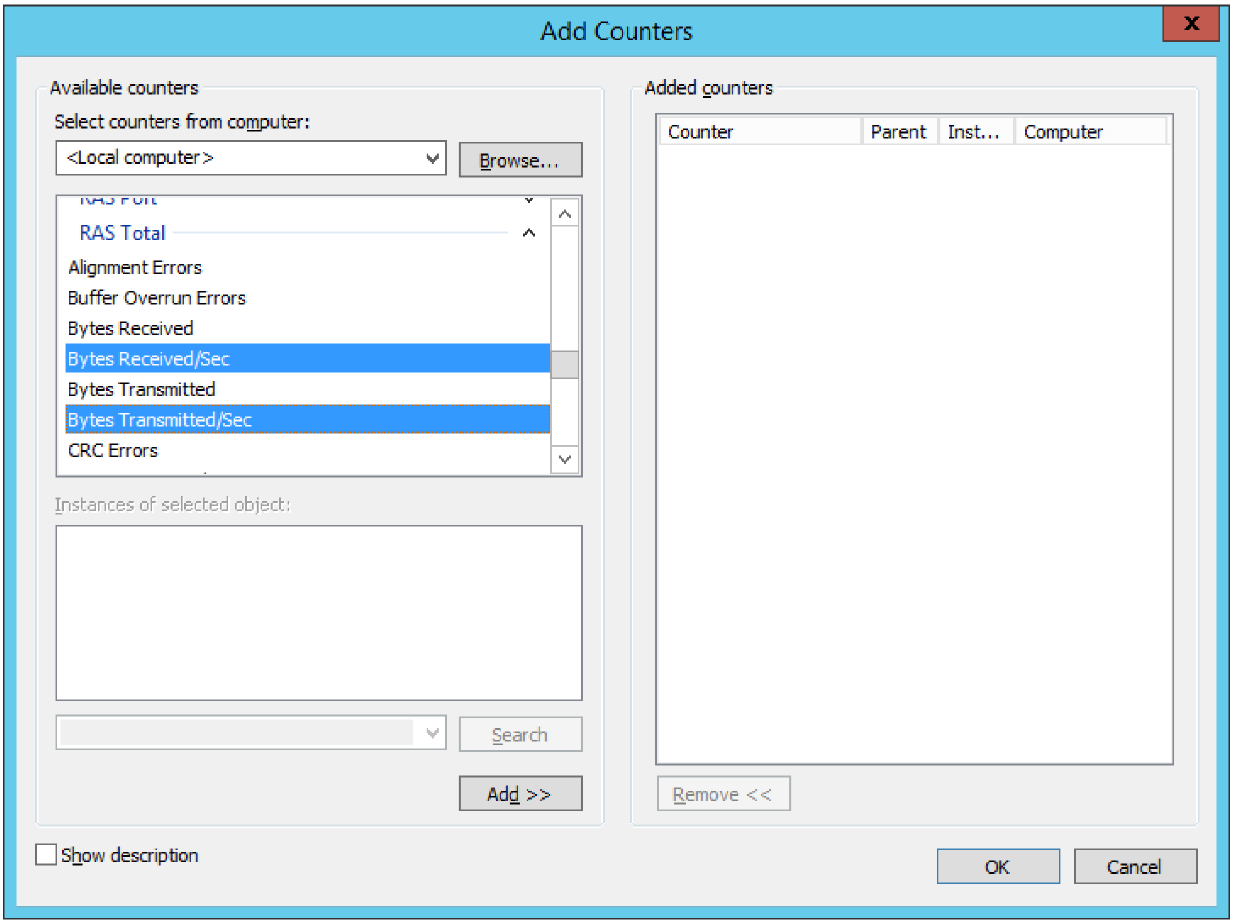
```
PS C:\> Get-AzureRmVirtualNetworkGatewayConnection -Name profx-gateway-connection2 -Resource-
GroupName profx-prod-rg

AuthorizationKey           :
VirtualNetworkGateway1     : Microsoft.Azure.Commands.Network.Models.PSVirtualNetworkGateway
VirtualNetworkGateway2     :
LocalNetworkGateway2       : Microsoft.Azure.Commands.Network.Models.PSLocalNetworkGateway
Peer                       :
ConnectionType             : IPsec
RoutingWeight              : 0
SharedKey                  : ####################################
ConnectionStatus           : NotConnected
EgressBytesTransferred     : 0
IngressBytesTransferred    : 0
ProvisioningState          : Succeeded
...
```

Miscellaneous issues

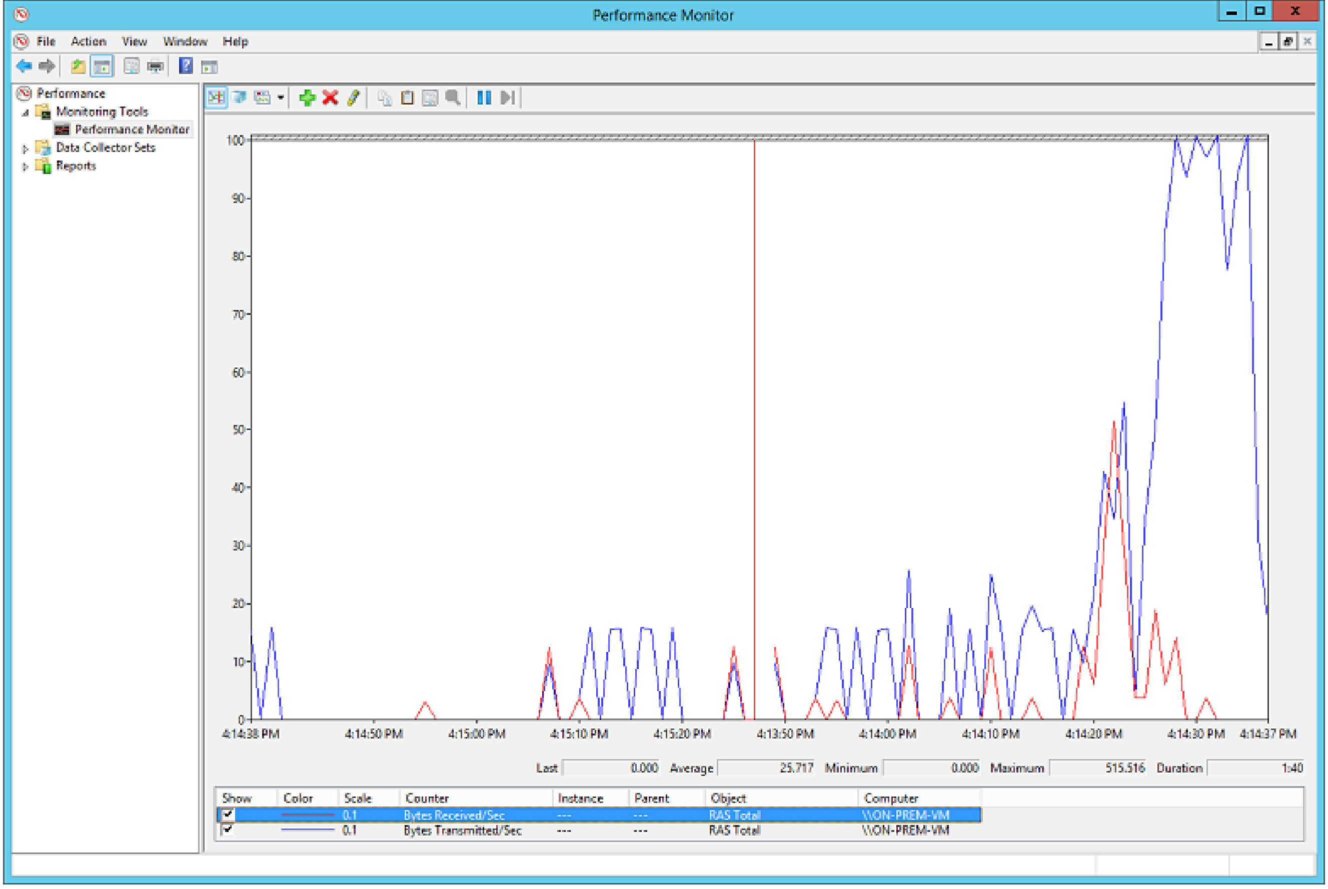
The following recommendations are useful for determining if there is an issue with Host VM configuration, network bandwidth utilization, or application performance:

Verify firewall configuration. Verify that the firewall in the guest operating system running on the Azure VMs in the subnet is configured correctly to allow permitted traffic from the on-premises IP ranges.

Verify that the volume of traffic is not close to the limit of the bandwidth available to the Azure VPN gateway. How to verify this depends on the VPN appliance running on-premises. For example, if you are using RRAS on Windows Server 2012, you can use Performance Monitor to track the volume of data being received and transmitted over the VPN connection. Using the *RAS Total* object, select the *Bytes Received/Sec* and *Bytes Transmitted/Sec* counters:



You should compare the results with the bandwidth available to the VPN gateway (from 100 Mbps for the Basic SKU to 1.25 Gbps for VpnGw3 SKU):



Last 0.000 Average 25.717 Minimum 0.000 Maximum 515.516 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	0.1	Bytes Received/Sec	---	---	RAS Total	\\ON-PREM-VM
☑	🟦	0.1	Bytes Transmitted/Sec	---	---	RAS Total	\\ON-PREM-VM

Verify that you have deployed the right number and size of VMs for your application load. Determine if any of the virtual machines in the Azure VNet are running slowly. If so, they may be overloaded, there may be too few to handle the load, or the load-balancers may not be configured correctly. To determine this, capture and analyze diagnostic information. You can examine the results using the Azure portal, but many third-party tools are also available that can provide detailed insights into the performance data.

Verify that the application is making efficient use of cloud resources. Instrument application code running on each VM to determine whether applications are making the best use of resources. You can use tools such as Application Insights.