Progress®
Kemp® LoadMaster®

Deployment Guide Microsoft Always On VPN

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Assumptions 6

Load Balancing Always On VPN 6

Prerequisites 6

Chapter 2: Template 8

Chapter 3: LoadMaster Global Settings 9

Enable Subnet Originating Requests Globally 9

Enable Check Persist Globally 10

Chapter 4: LoadMaster Virtual Services - IKEv2 11

Create a Virtual Service using a Template 12

IKEv2 UDP 500 Virtual Service Recommended API Settings (optional) 12

IKEv2 UDP 4500 Virtual Service Recommended API Settings (optional) 13

Configure Port Following for IKEv2 UDP Virtual Services 14

Port Following Configuration for IKEv2 UDP 500 14

Port Following Configuration for IKEv2 UDP 4500 14

Chapter 5: LoadMaster Virtual Services - SSTP 15

Create a Virtual Service using a Template 15

SSTP Passthrough Virtual Service Recommended API Settings (optional) 16

SSTP Offloaded Virtual Service Recommended API Settings (optional) 17

Configure TLS Offloading on the RRAS Server 17

Chapter 6: LoadMaster Virtual Services for NPS 19

Create a Virtual Service using a Template 19

NPS UDP 1812 Virtual Service Recommended API Settings (optional) 20

NPS UDP 1813 Virtual Service Recommended API Settings (optional) 20

Configure Port Following for NPS UDP Virtual Services 21

Port Following Configuration for NPS UDP 1812 21

Port Following Configuration for NPS UDP 1813 21

NPS Server Certificate Configuration 21

NPS Server Radius Configuration 23

Chapter 7: References 25

1

Introduction

Always On VPN is the replacement solution for Microsoft's popular DirectAccess remote access technology. It makes use of the native VPN client in the Windows 10 operating system to provide seamless, transparent, and always on remote access for mobile workers. Always On VPN is infrastructure independent and can be configured to use many popular VPN devices including Windows Server Routing and Remote Access Services (RRAS).

Intended Audience

This document is intended for Windows administrators tasked with implementing a scalable and highly-available Always On VPN infrastructure. The engineer should have a strong understanding of IPv4 networking and routing, as well as common VPN protocols such as Internet Key Exchange version 2 (IKEv2) and Secure Socket Tunnelling Protocol (SSTP). A fundamental understanding of Active Directory authentication, RADIUS, as well as certificates and Public Key Infrastructure is also helpful.

Document Purpose

This document provides guidance for configuring the LoadMaster load balancer to eliminate single points of failure and to provide scalability, redundancy, and fault tolerance for an Always On VPN deployment. This document uses a representative environment, which is described in detail later. It does not address all possible scenarios. For questions regarding unique configurations, contact the Progress Kemp support team.

About the Author

Richard Hicks is the founder and principal consultant of Richard M. Hicks Consulting, Inc. He is focused on

delivering enterprise mobility and security infrastructure solutions to customers of all sizes. Richard has more than 25 years of experience working in enterprise corporate computing environments and has designed and deployed secure remote access solutions for some of the largest companies in the world. He is also the author of *Implementing DirectAccess with Windows Server 2016* from Apress Media (ISBN: 978-1484220580). You can learn more about Richard by visiting https://www.richardhicks.com/.

Related Links

For details, see the following topics:

- Assumptions
- Load Balancing Always On VPN
- Prerequisites

Assumptions

This document assumes the reader has configured two Windows Server RRAS servers with two network interfaces, one in a perimeter or DMZ network, the other on the internal network. It should be noted that using two NICs is not a strict requirement. It is possible to configure Windows Server RRAS servers with a single network interface, if required. In addition, two Windows Server Network Policy Server (NPS) servers have been configured with a single network interface on the Internal network.

For details on recommended deployments, please reference the following link: https://directaccess.richardhicks.com/2018/01/22/always-on-vpn-protocol-recommendations-for-windows-server-routing-and-remote-access-service-rras/

Load Balancing Always On VPN

An enterprise Always On VPN deployment presents many opportunities to deploy LoadMaster products to provide scalability, fault tolerance, and deployment flexibility. The LoadMaster can be deployed to provide load balancing for the following Always On VPN infrastructure components.

1. **Routing and Remote Access Servers (RRAS) Servers** – An Always On VPN deployment may require more than one RRAS server to provide redundancy or to increase capacity to service more VPN connections than a single server is capable of.
2. **Network Policy Server (NPS) Servers** – To authenticate VPN connections, VPN servers are configured to forward authentication requests to an NPS server. Having more than one NPS server eliminates this single point of failure and may be required to support authentication for large scale deployments.
3. **Geographic Redundancy** – Unlike DirectAccess, Always On VPN has no concept of “multisite” configuration. To provide geographic redundancy, multiple VPN servers can be configured in various locations using a single, common public hostname. VPN client connections can then be routed to the most preferred location.

Prerequisites

Several prerequisites must be in place before proceeding with this documentation. In addition to the

assumptions outlined earlier in this document, it is assumed that the LoadMaster has been configured and that network connectivity to all networks has been validated. In addition, the following prerequisites must be in place before continuing.

- A public hostname for the VPN server that resolves to the IP address assigned to the VPN virtual service (or edge firewall if the LoadMaster is in a perimeter or DMZ network).
- An SSL certificate with a subject name that matches the VPN server's public hostname.
- Each VPN server must be configured to assign unique IP addresses to its clients. Using DHCP for VPN client address assignment when there is more than one VPN server in a cluster is not supported.
- An internal hostname for the NPS cluster that resolves to the IP address assigned to the NPS virtual service.

2

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

3

LoadMaster Global Settings

Before setting up the Virtual Services, the following global settings should be configured to support the workload.

Related Links

For details, see the following topics:

- Enable Subnet Originating Requests Globally
- Enable Check Persist Globally

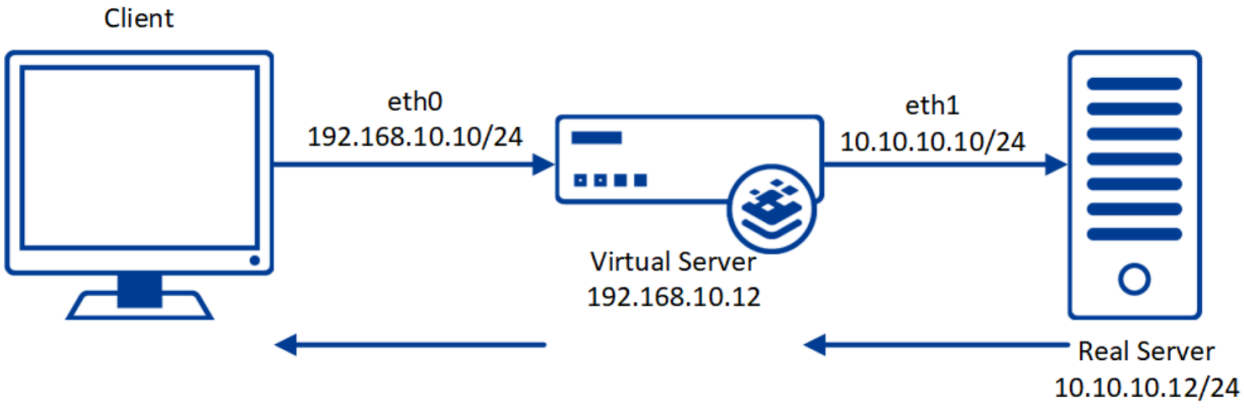
Enable Subnet Originating Requests Globally

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet), **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



In the diagram above, you can see the following details:

- Virtual Service on **eth0**: 192.168.10.10/24
- Virtual Server: 192.168.10.12
- Real Server on **eth1**: 10.10.10.10/24

With **Subnet Originating Requests** enabled, the Real Server sees traffic originating from 10.10.10.10 (LoadMaster **eth1** address) and responds directly.

If **Subnet Originating Requests** is disabled, the Real Server sees traffic originating from 192.168.10.10 (the Virtual Service address) and responds directly. In some environments this can lead to asymmetric routing which is why we recommend enabling **Subnet Originating Requests** unless specified otherwise

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.
2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

4

LoadMaster Virtual Services - IKEv2

IKEv2 communication takes place over UDP ports 500 and 4500. The initial connection is always made on UDP port 500. If a Network Address Translation (NAT) device is detected in the path, communication switches to using UDP port 4500. Since UDP is connectionless, special configuration is required to ensure that client connections are routed to the same Real Server.

Note: Windows limits the number of IPSec Security Associations (SAs) coming from a single IP address. Because of this limit, transparency must be set on the Virtual Service allowing the original client IP address to be seen on the VPN server. This requires that the default gateway on the VPN servers points to the LoadMaster for proper routing. If this configuration is not possible, the following workaround may resolve the issue:https://support.microsoft.com/en-us/help/2579729/ipsec-traffic-may-be-blocked-when-a-computer-that-is-running-windows-7

Note: For further information on transparency, refer to the Transparency Feature Description.

This guide contains a section on creating a Virtual Service in the WUI using a template. To configure the Virtual Services using the Application Programming Interface (API), refer to the RESTful API on the Documentation page.

Note: The recommended settings for the IKEv2 LoadMaster Virtual Services use the **Refresh Persist** option to ensure proper persistence for Microsoft Always On VPN clients. This functionality requires LoadMaster version 7.2.53 or higher.

The table in each section outlines the API settings and values. You can use this information when using the LoadMaster API and automation tools.

Related Links

For details, see the following topics:

- Create a Virtual Service using a Template
- Configure Port Following for IKEv2 UDP Virtual Services

Create a Virtual Service using a Template

To configure a Virtual Service using the application template, perform the following steps:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Enter the **Real Server Address**.
8. Confirm that the correct port is entered.
9. Click **Add This Real Server**.

Note: Do not forget to configure Port Following in Configure Port Following for IKEv2 UDP Virtual Services to ensure connections for IKEV2 are sent to the same Real Server. For more information, see the **Port Following** document on the Documentation page.

IKEv2 UDP 500 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	500
prot	udp
ForceL7	1
Transparent	1

API Parameter	API Value
Persist	src
PersistTimeOut	345600
RefreshPersist	1
Schedule	lc
CheckType	icmp

IKEv2 UDP 4500 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	4500
prot	udp
ForceL7	1
Transparent	1
Persist	src
PersistTimeOut	345600
RefreshPersist	1

API Parameter	API Value
Schedule	lc
CheckType	icmp

Configure Port Following for IKEv2 UDP Virtual Services

Port Following is required to ensure connections for IKEv2 UDP 500 and 4500 are sent to the same Real Server. To configure Port Following, see the following sections. For more information, see the **Port Following** document on the Documentation page.

Port Following Configuration for IKEv2 UDP 500

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** for the IKEv2 UDP 500 Virtual Service.
3. Expand **Advanced Properties**.
4. Select the IKEv2 UDP 4500 Virtual Service in the **Port Following** drop-down list.

Port Following Configuration for IKEv2 UDP 4500

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** for the IKEv2 UDP 4500 Virtual Service.
3. Expand **Advanced Properties**.
4. Select the **IKEv2 UDP 500** Virtual Service in the **Port Following** drop-down list.

5

LoadMaster Virtual Services - SSTP

SSTP communication takes place over TCP port 443. It uses TLS and can be load balanced in much the same way as an ordinary web server, with a few exceptions. It is generally recommended that the LoadMaster not be configured to terminate (offload) TLS, but instead passthrough encrypted connections directly to Real Servers. However, with some additional configuration, TLS offload can be enabled on the LoadMaster to reduce CPU utilization on Real Servers, if required.

This guide contains a section on creating a Virtual Service in the WUI using a template. To configure the Virtual Services using the Application Programming Interface (API), refer to the RESTful API on the Documentation page.

The table in each section outlines the API settings and values. You can use this information when using the LoadMaster API and automation tools.

Related Links

For details, see the following topics:

- Create a Virtual Service using a Template

Create a Virtual Service using a Template

To configure a Virtual Service using the application template, perform the following steps:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.

3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. (Required only for TLS/SSL Offload and ReEncrypt) Expand the **SSL Properties** section.
6. (Required only for TLS/SSL Offload and ReEncrypt) Select the certificate to use in the **Available Certificates** and click the **arrow >** to move it to **Assigned Certificates**.
7. Expand the **Real Servers** section.
8. In the **HTTP1.1/Host** field, enter the public hostname/URL of the VPN and click **Set Host**.
9. Click **Add New**.
10. Enter the **Real Server Address**.
11. Confirm that the correct port is entered.
12. Click **Add This Real Server**.

SSTP Passthrough Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOrg	1
Persist	src
PersistTimeOut	300
Schedule	lc
CheckType	tcp
CheckPort	443
CheckURL	/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/
CheckStatusCode	401
UseHTTP/1.1	1
HTTPMethod	Head

SSTP Offloaded Virtual Service Recommended API Settings (optional)

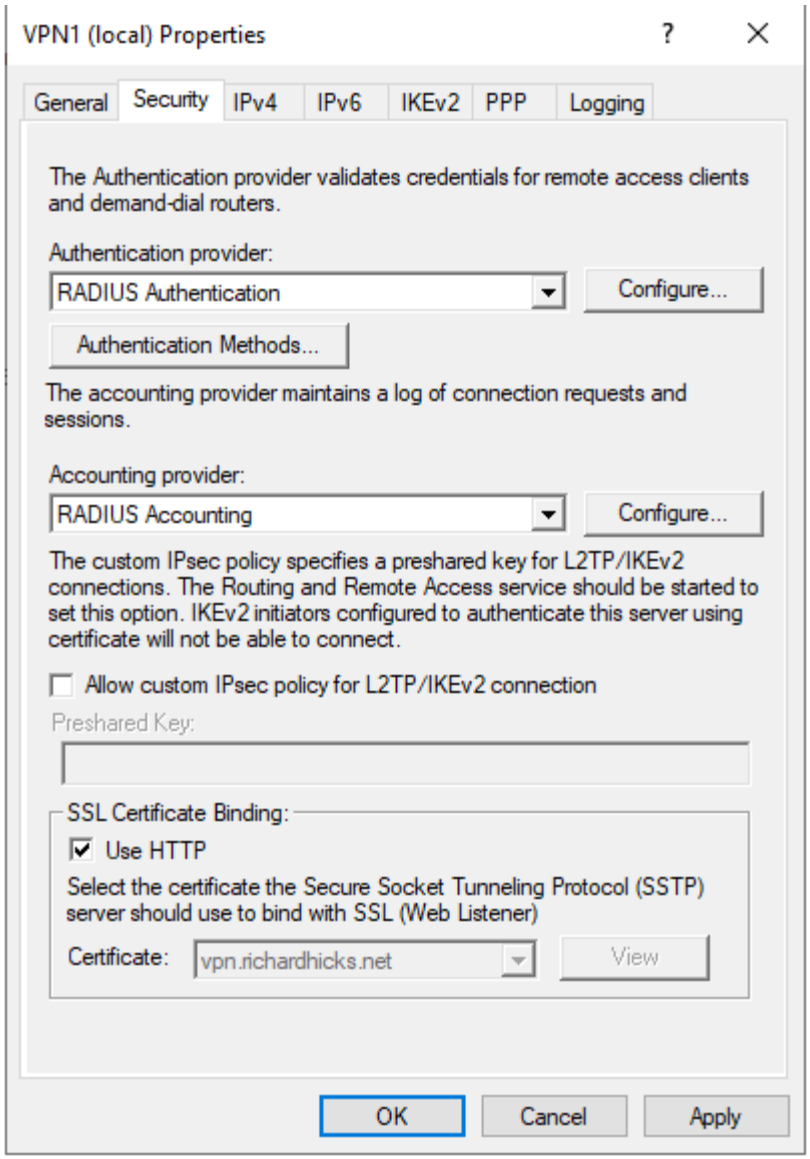
This table outlines the API parameters and values set using the Progress Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Persist	src
PersistTimeOut	300
Schedule	lc
SSLAcceleration	1
TLSType	7
CheckType	HTTP
CheckURL	/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/
CheckStatusCode	401
UseHTTP/1.1	1
HTTPMethod	Head

Configure TLS Offloading on the RRAS Server

On the Windows RRAS server, open the Remote Access Management console (rrasmgmt.msc) and perform the following steps:

1. Right-click the VPN server and select **Properties**.
2. Select the **Security** tab.
3. Select the public SSL certificate in the **SSL Certificate Binding** box.
4. Select the option to **Use HTTP**.
5. Click **Ok**.
6. Click **Yes** when prompted to restart the service.
7. Repeat these steps on each RRAS server in the cluster.



Note: It is assumed that the public SSL certificate is installed on the RRAS server when performing the steps above. In some cases, installing the public SSL certificate on the RRAS server may not be possible. In this scenario the administrator must manually configure the RRAS server to support SSL offload for SSTP. For further details, refer to the following page: Always On VPN SSTP Load Balancing and SSL Offload.

6

LoadMaster Virtual Services for NPS

NPS communication takes place over UDP ports 1812 and 1813. Authentication requests on UDP port 1812 and accounting requests on port UDP 1813. Both of these connections must be sent to the same NPS server. Since UDP is connectionless, special configuration is required to ensure that client connections are routed to the same Real Server.

This guide contains a section on creating a Virtual Service in the WUI using a template. To configure the Virtual Services using the Application Programming Interface (API), refer to the RESTful API on the Documentation page.

The table in each section outlines the API settings and values. You can use this information when using the LoadMaster API and automation tools.

Related Links

For details, see the following topics:

- Create a Virtual Service using a Template
- Configure Port Following for NPS UDP Virtual Services

Create a Virtual Service using a Template

To configure a Virtual Service using the application template, perform the following steps:

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.

3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.
7. Enter the **Real Server Address**.
8. Confirm that the correct port is entered.
9. Click **Add This Real Server**.

Note: Do not forget to configure Port Following in Configure Port Following for IKEv2 UDP Virtual Services to ensure connections for IKEV2 are sent to the same Real Server. For more information, see the **Port Following** document on the Documentation page.

NPS UDP 1812 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	1812
prot	udp
ForceL7	1
Persist	src
PersistTimeOut	300
Schedule	lc
CheckType	icmp

NPS UDP 1813 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Progress Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	1813

API Parameter	API Value
prot	udp
ForceL7	0
Persist	src
PersistTimeOut	300
Schedule	lc
CheckType	icmp

Configure Port Following for NPS UDP Virtual Services

Port Following is required to ensure connections for IKEv2 UDP 1812 and 1813 are send to the same Real Server. To configure Port Following, see the sections below.

Port Following Configuration for NPS UDP 1812

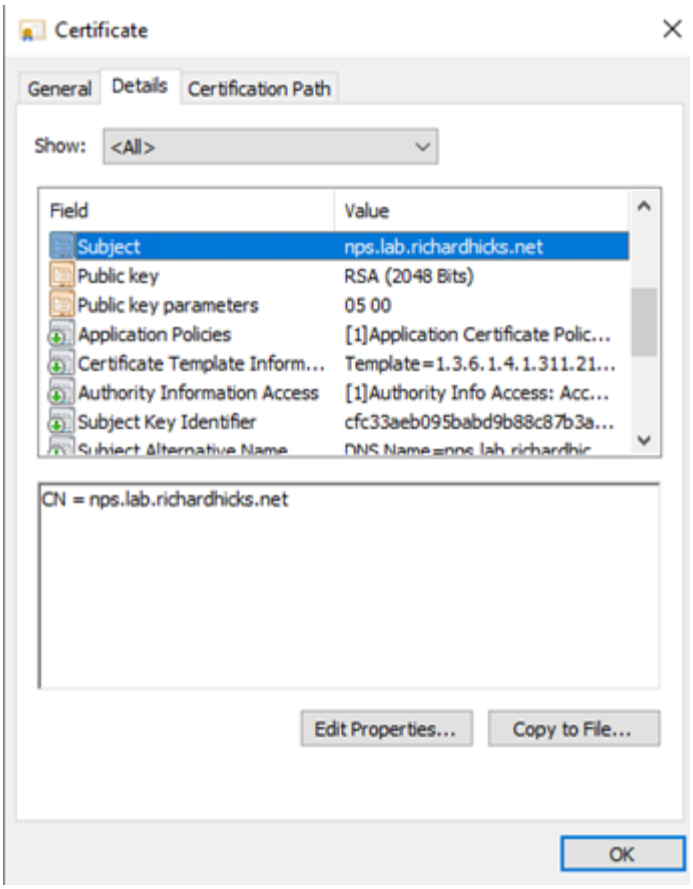
1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** for the NPS UDP 1812 Virtual Service.
3. Expand **Advanced Properties**.
4. Select the **NPS UDP 1813** Virtual Service in the **Port Following** drop-down list.

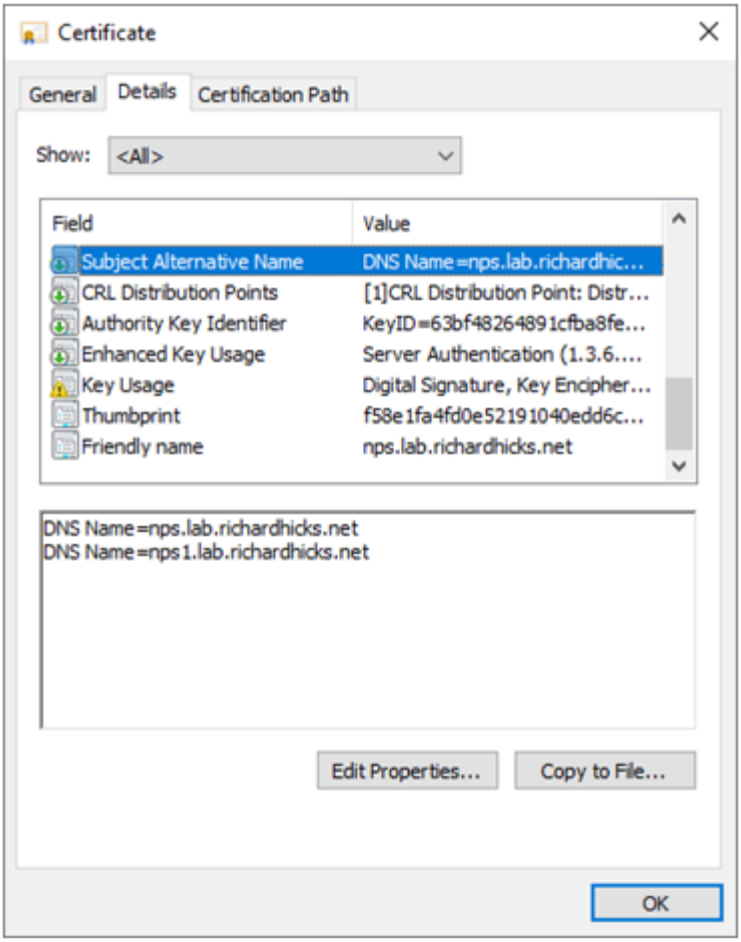
Port Following Configuration for NPS UDP 1813

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** for the NPS UDP 1813 Virtual Service.
3. Expand **Advanced Properties**.
4. Select the **NPS UDP 1812** Virtual Service in the **Port Following** drop-down list.

NPS Server Certificate Configuration

To support LoadMaster load balancing for NPS, the certificate installed on the NPS server must be configured to use the cluster Fully Qualified Domain Name (FQDN) as the subject name on the certificate, with the Subject Alternative Name fields including the FQDNs of both the cluster and server names.

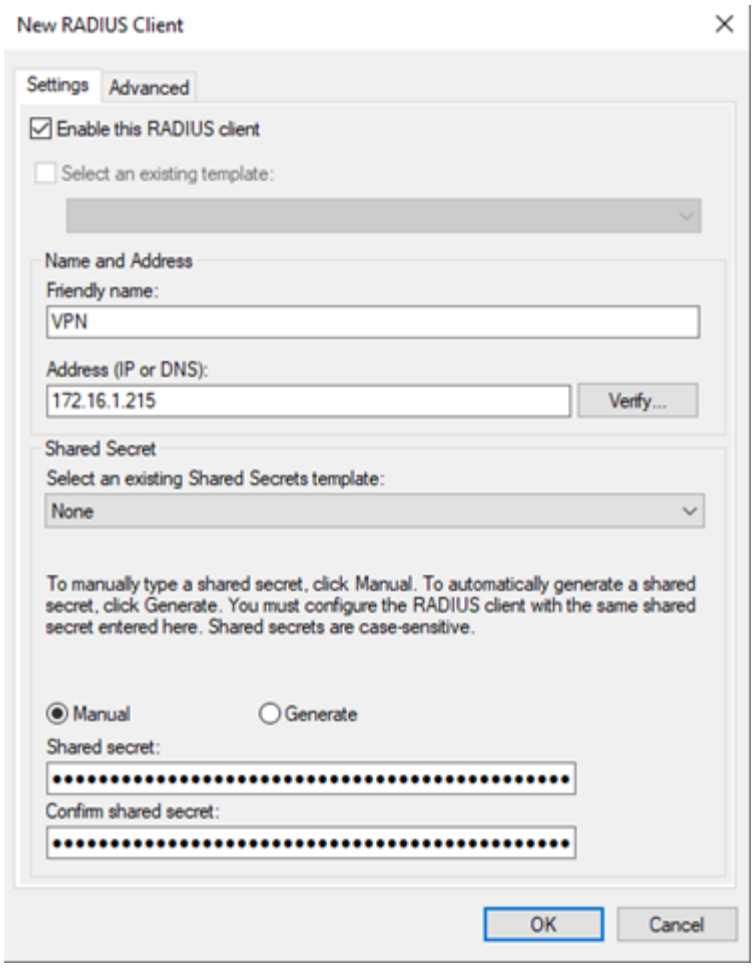

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
nps.lab.richardhicks.net
Public key
RSA (2048 Bits)
Public key parameters
05 00
Application Policies
[1]Application Certificate Polic...
Certificate Template Inform...
Template=1.3.6.1.4.1.311.21...
Authority Information Access
[1]Authority Info Access: Acc...
Subject Key Identifier
cfc33aeb095babd9b88c87b3a...
CN = nps.lab.richardhicks.net
Edit Properties...
Copy to File...
OK



NPS Server Radius Configuration

When a LoadMaster is load balancing NPS, the source IP address of the RADIUS authentication and accounting requests is the Virtual IP Address (VIP) assigned to the virtual service. A RADIUS client must be configured in NPS to allow authentication and accounting requests to be processed. Open the NPS management console and perform the following steps.

1. Expand **RADIUS Clients and Servers**.
2. Right-click **RADIUS Clients** and select **New**.
3. Enter a friendly name for the new RADIUS client.
4. Enter the VIP of the NPS virtual service in the **Address (IP or DNS)** field.
5. Enter and confirm the shared secret used between the NPS and VPN servers.
6. Click **Ok**.
7. Repeat the steps above on each NPS server in the cluster.


New RADIUS Client
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
VPN
Address (IP or DNS):
172.16.1.215
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel

7

References

Some resources on Microsoft Always On VPN are listed below:

The Microsoft Always On VPN document can be found on the Documentation page.

Microsoft Windows 10 Always On VPN

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/

Microsoft Windows 10 Always On VPN Deployment Guide

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy

Richard Hicks Enterprise Mobility Blog

https://directaccess.richardhicks.com/