How to add RADIUS Shared Secret in NetScaler for RADIUS deployments?

Why RADIUS shared secret?

In a typical RADIUS deployment where a RADIUS server is accessed by RADIUS clients or by RADIUS proxy a shared secret is maintained by the participating nodes to achieve security. This shared secret is pre-configured in these RADIUS nodes before they start communication with each other. The fact that this shared secret is not sent over the network anytime, provides security and helps in authenticating the RADIUS communications. It eliminates the possibility of intruders snooping on an unsecure network which is quite critical in this case, as user's passwords are transmitted during RADIUS communications.

How does RADIUS shared secret work?

Let us take the example of RADIUS client and RADIUS server in a network. As already mentioned a RADIUS shared secret key is configured on RADIUS client and RADIUS server. Now, if RADIUS client sends a request to RADIUS server, it validates the client messages using the shared secret. If the RADIUS client doesn't have a valid shared secret, then the message is silently discarded. If the RADIUS client is valid, then RADIUS server performs further processing of the message and proceeds with communication. RADIUS shared secret also helps to identify if the message has been modified during transit. It is also used to encrypt some of the RADIUS attributes like passwords which are highly sensitive information.

Given the fact that this RADIUS secret key plays a vital role in secure communication, it should be selected such that it is large, at least 16 octets to protect against search attacks and should not be guessable.

How RADIUS shared secret is used in NetScaler?

Use case - RADIUS Load Balancing

The concept of shared secret applies to RADIUS Load balancers also. In this case, a RADIUS Load balancer which load balances RADIUS client messages to RADIUS servers should have a shared secret configured in RADIUS server and RADIUS Load balancer on the server side and a shared secret should be configured in RADIUS client and RADIUS Load balancer on the client side.

For more information on RADIUS LB in NetScaler refer - https://docs.citrix.com/en-us/netscaler/11/traffic-management/load-balancing/load-balancing-persistence/radius-persistence.html

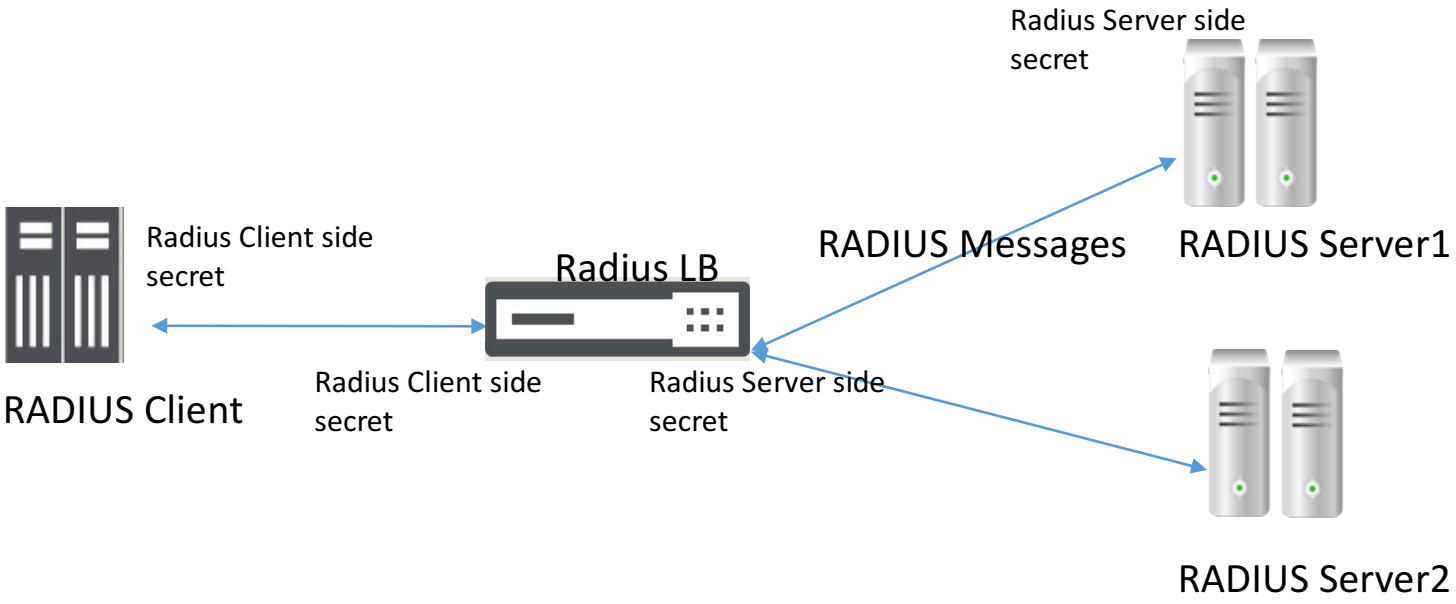


Fig: RADIUS LB with RADIUS shared secret

Use case- Subscriber Management

When NetScaler receives RADIUS accounting messages from RADIUS proxy (which is consumed and used to query PCRF to get subscriber information using Gx interface), NetScaler uses a RADIUS listener service. RADIUS shared secret has to be configured for RADIUS listener service in NetScaler and also in RADIUS proxy for proper RADIUS communication.

For more information on Telco Subscriber management - https://docs.citrix.com/en-us/netscaler/11/solutions/netscaler-support-for-telecom-service-providers/lsn-telco-subscriber-management.html

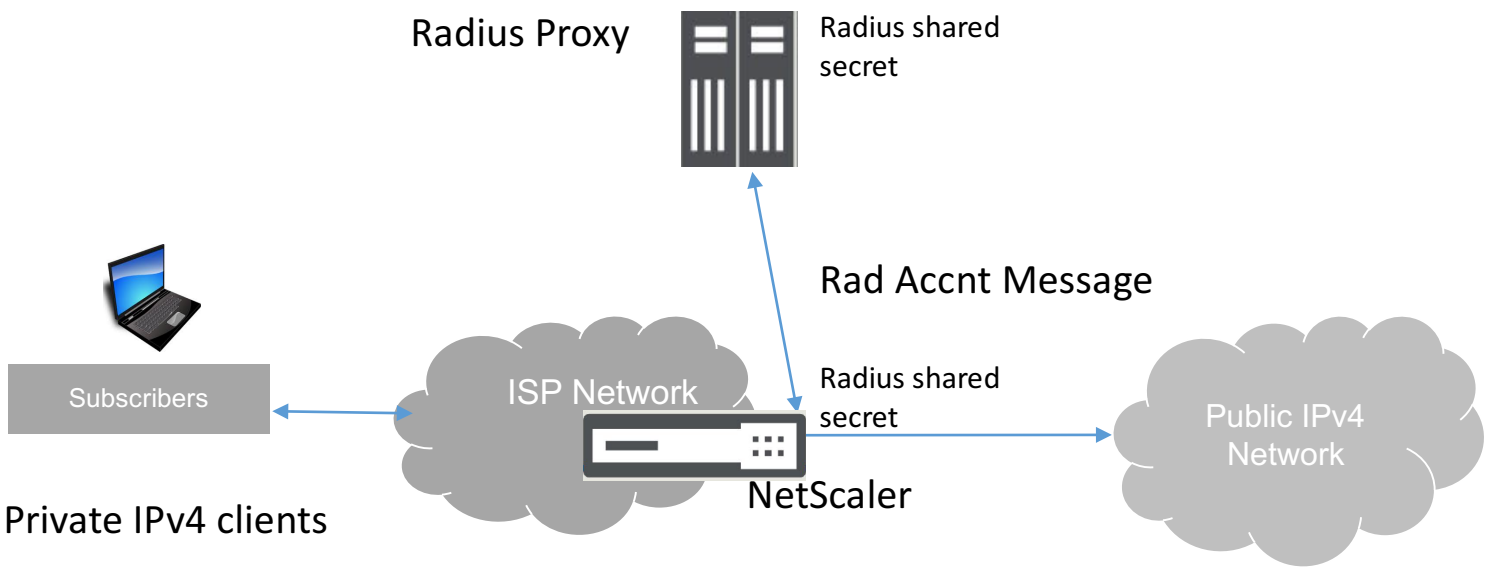
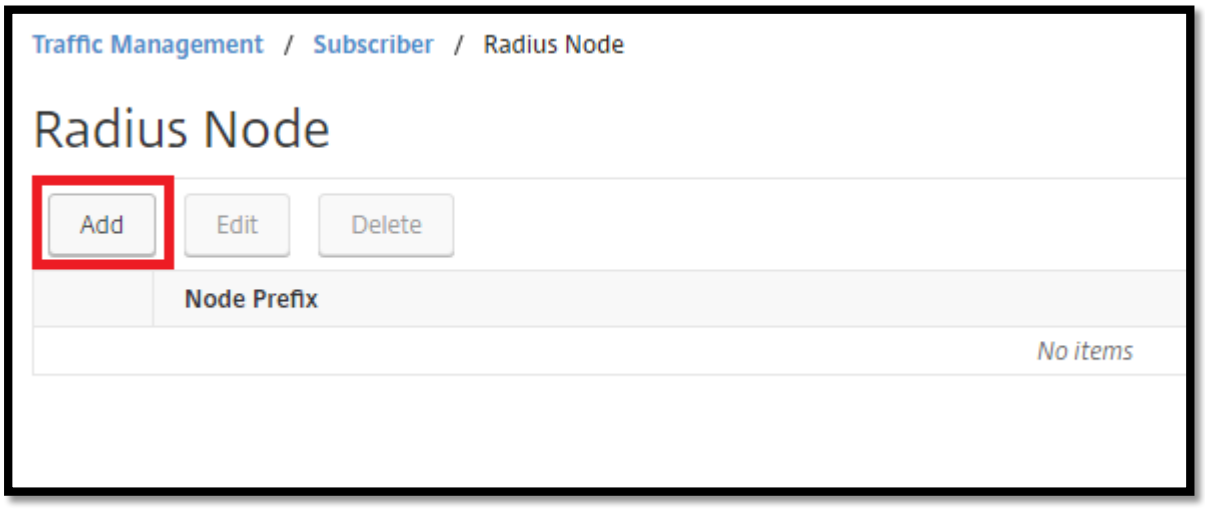


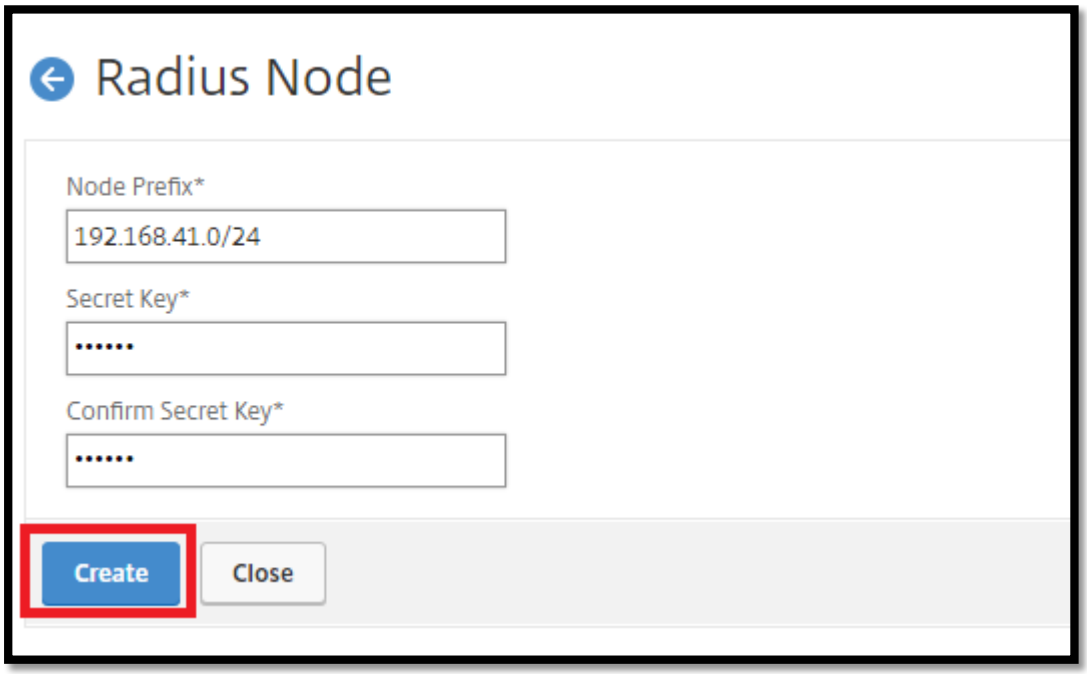
Fig: RADIUS Listener service with RADIUS shared secret

How to configure RADIUS shared secret in NetScaler?

For configuring RADIUS node under configuration utility,

Navigate to Configuration > Traffic Management > Subscriber > Radius Node





For add RADIUS shared secret in command prompt the below mentioned CLI has be used,

> add radiusNode <Client or ServerPrefix/Subnet> -radKey <client or serverkey> - key that is shared with the RADIUS node at the other end

For eg. add radiusNode <client network> -radkey **clientkey123** - key that is shared with Radius client

Default Radius shared secret can be configured using 0.0.0.0/0 Subnet.

The same configuration above applies for RADIUS listener service also.