Validação de certificado SSL - Redis

O Redis não tem suporte integrado para SSL. É recomendável o uso de software de encapsulamento, como stunnel, para habilitar SSL para o servidor do Redis. A configuração do stunnel envolve a especificação da porta para a aceitação de uma conexão segura e o certificado a ser usado como o certificado do servidor.

Para habilitar SSL com o cliente Redis SSL, a impressão digital do certificado deve ser adicionada no Painel de controle do Archer. O Archer está qualificado para o servidor stunnel. O servidor do stunnel pode ser configurado para fazer uma validação de certificado completa, inclusive a validação da cadeia de certificados, ou uma validação de nomes. Para o certificado do servidor, o Painel de controle do Archer faz uma validação estrita do certificado apresentado pelo servidor como parte do handshake. Para obter mais informações sobre como usar o stunnel com o Redis, consulte a documentação do site do Redis.

Verifique se o certificado que é usado com o servidor do stunnel atende às seguintes condições:

- A cadeia de certificados é confiável para o Painel de controle do Archer e para todos os serviços e servidores da Web do Archer. Todas as autoridades intermediárias e a autoridade de root devem ser confiáveis em todos os servidores.
- O certificado é emitido com o nome correto do indivíduo. Não pode haver nenhuma disparidade de nome ou qualquer outro erro de política SSL.
- O certificado deve ser válido e não expirado.

Você pode testar o servidor que se conecta no Painel de controle do Archer. Para obter mais informações, consulte "Testando a conexão em cache" na Ajuda do Painel de controle do Archer.