Q.A para CERTIFICADOS DE TELEFONE CUCM (LSC/MIC)

Contents

Introduction

Este documento aborda algumas das perguntas e respostas dos certificados do telefone do Cisco Unified Communications Manager (CUCM). Aqui está uma exibição rápida dos certificados de telefone.

Certificado instalado pelo fabricante (MIC):

Como o nome indica, os telefones são pré-instalados com o MIC e isso não pode ser excluído/modificado pelos administradores. Os certificados da autoridade de certificação (CA)

CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA e Cisco Manufacturing CA SHA2 são pré-instalados no CUCM para confiar no MIC. O MIC não pode ser usado depois que a validade expirar, pois a CA do MIC não pode ser gerada novamente,

Certificado localmente significativo (LSC):

O LSC possui a chave pública para o telefone IP da Cisco, que é assinado pela chave privada da Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF). Por padrão, ele não está instalado no telefone. O administrador tem controle total sobre o LSC. O certificado de CA CAPF pode ser regenerado por sua vez e pode emitir novo LSC para os telefones sempre que necessário.

Quais são os usos comuns de certificados de telefone?

Aqui estão alguns usos comuns para certificados de telefone

Entre CAPF e telefone para instalação/atualização, exclusão ou solução de problemas

O telefone estabelece a conexão com o CAPF para instalar/atualizar, excluir ou solucionar problemas de certificado no telefone. O certificado de telefone é usado para estabelecer a conexão com o CAPF quando o Modo de autenticação sob a função de proxy da autoridade de certificação (CAPF) Informações definidas como Por Certificado existente (Precedência ao LSC) ou Por Certificado existente (Precedência ao MIC).

Por certificado existente (precedência ao LSC): o telefone usa o LSC para autenticar com o CAPF. Ele usará o MIC se o LSC não estiver instalado. A instalação falha com o motivo "LSC inválido" se houver problemas com o certificado usado. Por exemplo, a CA assinada para o LSC não está disponível no CAPF Trust. Atualize o modo de autenticação usando outro método de certificado ou uma string nula para tais casos de falha.

Por certificado existente (precedência ao MIC): O telefone usa MIC para autenticar com CAPF.

Entre o CallManager e o telefone para a conexão TLS (Transport Layer Security)

O telefone usa LSC ou MIC para estabelecer a conexão TLS com o CallManager. O CallManager validará o certificado apresentado pelo telefone marcando CallManager-trust. O respectivo certificado CAPF deve estar disponível no CallManager-trust para LSC e CAs de fabricação da Cisco para MIC.

Entre o servidor de telefone e autenticação para autenticação 802.1x

Os certificados de CA de produção/CAPF são carregados em servidores de autenticação, como o Cisco Secure Access Control Server (ACS) ou Identity Services Engine (ISE). O servidor de autenticação usa os certificados carregados para autenticar o telefone quando ele apresenta seu certificado (LSC ou MIC).

Para autenticação baseada em certificado entre o telefone e o Cisco Adaptive

Security Appliance (ASA) para VPN

Os certificados de CA de fabricação/CAPF são carregados no ASA, quando o telefone apresenta o LIC/MIC, o ASA valida-o verificando sua confiança.

Quando o LSC e o MIC estão presentes, há alguma maneira de selecionar o LSC ou o MIC explicitamente para conexões?

Nenhuma opção para selecionar se LSC ou MIC para as conexões. Se o LSC estiver instalado, o telefone usará o LSC. O telefone usa o MIC se o LSC não estiver instalado .

Entrada do console quando o LSC não está presente:

SEGUNDO: -PXY_NO_LSC: Nenhum LSC para [SCCP], tentará o MIC

Entrada do console quando o LSC está presente:

SEGUNDO: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC]

A seleção de LSC ou MIC só é possível entre CAPF e Telefone para instalação/atualização, exclusão ou solução de problemas.

Por que os telefones instalados do LSC com perfil seguro não estão sendo registrados ao migrar para um novo cluster?

Isso pode acontecer para os telefones que já têm um LSC do cluster OLD. Quando o MIC e o LSC estão presentes, o LSC é usado para estabelecer a conexão TLS. O TLS não pode ser estabelecido porque o novo CUCM não tem a CA para este LSC em sua confiança do CallManager.

Os registros do console mostram qual certificado é usado para estabelecer o TLS. A entrada abaixo mostra que LSC é usado.

3469 NÃO 00:01:31.935298 SECD: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC], cifra [AES256-SHA:AES128-SHA]

SSL3_Alert com "CA desconhecida" para casos com falha em logs de console :-

3486 ERRO 00:01:31.938954 SECD: -STATE_SSL3_ALERT: Alerta SSL3 [lido]:[fatal]:[CA desconhecida

Uma das maneiras de resolver esse problema é registrar o telefone usando um perfil não seguro e excluir o LSC existente. Instale o LSC do novo cluster e registre o telefone usando o perfil seguro. Também é possível que o telefone com perfil seguro esteja registrado usando o MIC sem instalar o LSC.

Énecessário ter o LSC instalado para que os telefones o

registrem usando o perfil seguro autenticado ou criptografado?

Não. Se o LSC não estiver instalado, o telefone usará o MIC para estabelecer a conexão TLS com o CUCM.

4878 AVI 15:47:34.756063 SECD: -PXY_NO_LSC: Sem LSC para [SCCP], tenta MIC.

Éobrigatório que o modo de segurança do dispositivo no respectivo perfil de segurança do dispositivo seja autenticado ou criptografado para instalar/atualizar/excluir um LSC?

Ele não é obrigatório; ele pode ser feito usando o padrão de perfil não seguro padrão também onde o modo de segurança do dispositivo não é seguro.

Éobrigatório que o cluster esteja no modo misto para instalar o LSC no telefone?

Não é obrigatório. A instalação/exclusão do LSC pode ser feita mesmo quando o modo de segurança do cluster não é seguro.

Como testar rapidamente se há um problema com o LSC usado pelo telefone?

Exclua o LSC em um dos telefones acessando a página do administrador do telefone. Isso força o telefone a usar o MIC. Se tudo estiver bem com o MIC, continue a solução de problemas com o LSC.

Como obter os certificados de telefone para solução de problemas?

Defina a operação do certificado para solução de problemas no dispositivo/telefone. Pressione Salvar e depois Aplicar configuração. Aguarde para ver o Status da operação do certificado para **solucionar problemas de sucesso**. Coletar registros de **funções de proxy da autoridade de certificação da Cisco** da Ferramenta de Monitoramento em Tempo Real (RTMT). Contém os certificados do telefone.

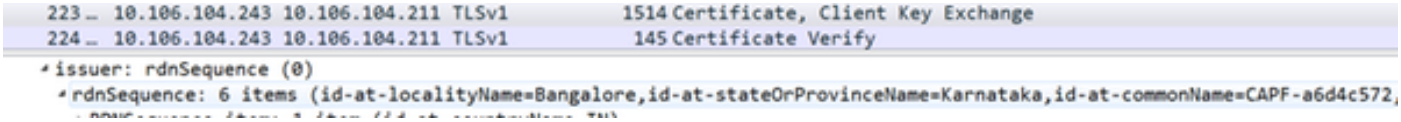
Como verificar a partir das capturas de pacotes se o LSC ou o MIC do telefone é usado para estabelecer a conexão TLS com o CallManager?

Colete as Capturas de Pacotes cobrindo a reinicialização do Telefone.

Verifique a mensagem Certificate, Client key Exchange (Certificado, chave do cliente de troca). Verifique o certificado enviado do telefone IP.

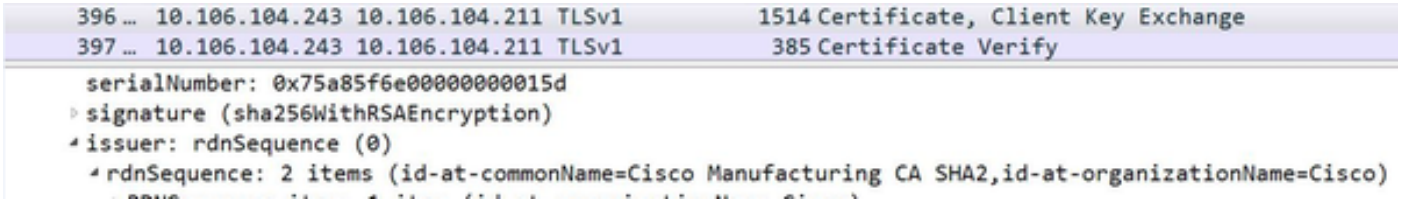
Exemplo de LSC:

Para o LSC, o CN do CAPF é visto no campo emitente. A respectiva raiz CAPF deve estar presente na confiança do CallManager.



Exemplo de MIC:

Para o MIC, CA de manufatura da Cisco no campo emitente. A AC raiz respectiva deve estar presente na confiança do CallManager.



Qual é o significado do Modo de Autenticação nas Informações da Função de Proxy da Autoridade de Certificação (CAPF)? Algum significado para a conexão TLS entre o CUCM e o Telefone?

Não é mais do que um método de autenticação entre o Telefone e o CAPF para instalar/atualizar/excluir e solucionar problemas de operações. Ele não tem importância para a conexão TLS entre o CUCM e o telefone.

Quais são as operações de LSC básicas que os telefones devem considerar após a regeneração do certificado CAPF?

Esta seção aborda o cenário de ociosidade em que nenhuma CA offline é usada para emitir o LSC.

Conexão TLS com CallManager

Certifique-se de instalar o novo LSC no telefone antes de excluir o certificado CAPF anterior do CallManager-trust. A exclusão do certificado CAPF anterior seguida de uma reinicialização do serviço CallManager faz com que os problemas de registro nos telefones que possuem o LSC emitido por este certificado CAPF sejam solucionados.

Operações LSC com CAPF-Trust

Certifique-se de instalar o novo LSC no telefone antes de excluir o certificado CAPF anterior do CAPF-trust. Operações LSC como instalar/excluir usando o modo de autenticação **pelo Certificado Existente (Precedência para LSC)** falha com erro **LSC inválido** para os telefones que possuem o LSC emitido por este Certificado CAPF.

Entre o servidor de telefone e autenticação para autenticação 802.1x

Certifique-se de não excluir o certificado CAPF anterior do servidor de autenticação até que o novo certificado CAPF seja carregado e o telefone obtenha o LSC emitido pelo novo CAPF.

Entre ASA e telefone

Certifique-se de não excluir o certificado CAPF anterior do ASA até que o telefone obtenha o novo LSC e carregue o novo certificado CAPF CA para o ASA.

Consulte a Regeneração de Certificado para ver as etapas a serem seguidas para gerar novamente o Certificado CAPF.

Informações Relacionadas

- Certificados de telefone IP da Cisco e comunicações seguras
- Guia de design de telefonia IP para 802.1X
- Guia de segurança do Cisco Unified Communications Manager