Guia completo do Jabber Como para a validação certificada

Índice

Introdução

Este documento combina diversos recursos Cisco em um guia completo, Como unificado que seja usado a fim executar todas as exigências para a validação certificada no Jabber de Cisco. Isto é necessário porque Cisco Jabber exige agora o uso da validação certificada a fim estabelecer conexões seguras com server. Esta exigência envolve muitas mudanças que puderam ser exigidas para ambientes de usuário.

> Nota: Este guia é para disposições dos em-locais somente. Não há atualmente nenhuma mudança exigida para distribuições de serviço da nuvem, porque são validados contra o Certificate Authority (CA) público.

Que clientes do Jabber são afetados por esta mudança?

Está aqui uma tabela que aliste todos os clientes que executam a validação certificada:

Tabela 1

Clientes de desktop	Clientes do móbil e da tabuleta

Jabber para a versão 9.2 de Macintosh (setembro 2013)	Jabber para a versão 9.5 do iPhone (outubro 2013)
Jabber para a versão do Windows 9.2.5 de Microsoft (MS) (setembro 2013)	Jabber para a versão 9.6 do iPhone e do iPa (novembro 2013) Jabber para a versão 9.6 de Android (dezem 2013)

Que faz este meio para o ambiente do Jabber?

Quando você instala ou elevação a todo o cliente alistado na **tabela 1**, a validação certificada imperativa com server está usada para conexões seguras. Essencialmente, quando os clientes do Jabber tentam fazer agora uma conexão segura, os server Cisco atual Jabber com Certificados. Cisco Jabber então tentativas de validar aqueles Certificados contra a loja do certificado do dispositivo. Se o cliente não pode validar o certificado, alerta-o confirmar que você quer aceitar o certificado, e o coloca em sua loja da confiança da empresa.

Que Certificados são exigidos?

Estão aqui uma lista de server de em-locais e os Certificados que apresente a Cisco o Jabber a fim estabelecer uma conexão segura:

Tabela 2

Servidor	Certificado
Cisco Unified Presence	HTTP (Tomcat) XMPP
Gerente das comunicações unificadas de Cisco IM e presença	HTTP (Tomcat) XMPP
Gerente das comunicações unificadas de Cisco	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Server das reuniões do WebEx de Cisco	HTTP (Tomcat)

Estão aqui alguns pontos importantes a notar:

- Aplique a atualização a mais recente do serviço (SU) para o Cisco Unified Presence (COPO) ou o gerente das comunicações unificadas de Cisco (CUCM) IM e presença antes que você comece o processo de assinatura do certificado.
- Os Certificados exigidos aplicam-se a todas as versões de servidor. Por exemplo, versão 8.x do COPO e CUCM IM e presente da versão 9.x e mais recente da presença o cliente com protocolo elástico da Mensagem e da presença (XMPP) e Certificados HTTP.
- Cada nó em um conjunto, assinantes e editores, executa um serviço de Tomcat e pode apresentar o cliente com um certificado HTTP. Planeie assinar os Certificados para cada nó no conjunto.
- A fim fixar o Session Initiation Protocol (SIP) que sinaliza entre o cliente e o CUCM, use o registro da função do proxy da autoridade de certificação (CAPF).

Que métodos estão disponíveis para a validação certificada?

Há atualmente diversos métodos da validação de certificação que podem ser usados.

Método 1: O clique dos usuários simplesmente **aceita a** todos os pop-up do certificado. Esta pôde ser a maioria de solução ideal para ambientes menores. Se você clique **aceita**, os Certificados estão colocados na loja da confiança da empresa no dispositivo. Depois que os Certificados são colocados na loja da confiança da empresa, os usuários estão alertados já não quando registram no cliente do Jabber nesse dispositivo local.

Método 2: Os Certificados exigidos (**tabela 2**) são transferidos dos servidores individuais (à revelia, estes são certificados auto-assinados) e instalados na loja da confiança da empresa do dispositivo de usuário. Esta pôde ser a solução ideal se seu ambiente não tem o acesso a CA privado ou público para a assinatura do certificado.

Diversos métodos podem ser usados a fim empurrar estes Certificados para usuários, mas um método rápido é empregar o uso do registro de Microsoft Windows:

1. De uma das máquinas, aceite todos os Certificados que são apresentados para jabber na loja da confiança da empresa.
2. A fim verificar que os Certificados estam presente, incorpore o **comando Certmgr.msc** e navegue a EnterpriseTrust **> a Certificados.**
3. Abra **Regedit** com um comando da **corrida** e navegue a **HKCU > software > Microsoft > SystemCertificates > confiança > Certificados**.
4. Clicar com o botão direito e exporte o dobrador de Certifates no registro como um arquivo **.reg**.
5. Elimine este arquivo através do objeto da política do grupo (GPO) a todos os usuários (ou ao outro método preferido).

Isto termina a instalação de Certificados de confiança da empresa para o Jabber, e os usuários são alertados já não.

Método 3: Um público ou CA privado (**tabela 2**) assinam todos os Certificados exigidos. Este é o método recomendada de Cisco. Este método exige que uma solicitação de assinatura de certificado (CSR) está gerada para cada um dos Certificados, é assinado, re-transferido arquivos pela rede ao server, e importado então às autoridades de certificação do root confiável a loja em dispositivos de usuário. Veja a **geração um CSR** e **como eu obtenho Certificados às lojas do certificado dos dispositivos de usuário?** seções deste documento para mais informação.

> Nota: No caso de CA público, o certificado de raiz deve já estar na loja da confiança do cliente.

Éimportante recordar que o público CA exige tipicamente CSR a fim se conformar aos formatos específicos. Por exemplo, CA público pôde somente aceitar CSR isso:

- São Base64-encoded
- Não contenha determinados caráteres, tais como o @&! , na organização, na unidade organizacional (OU), ou nos outros campos
- Use comprimentos de bit específicos na chave pública para o server

Igualmente, se você submete CSR dos nós múltiplos, o público CA pôde exigir que a informação é consistente em todos os CSR.

A fim impedir edições com seus CSR, reveja as exigências do formato de CA público a que você

planeia submeter os CSR. Assegure-se de então que a informação que você incorpora quando você configura seu server se conforma ao formato que CA público exige.

Está aqui uma exigência que possível você pôde encontrar:

Um certificado pelo FQDN: Algum sinal do público CA somente um certificado pelo nome de domínio totalmente qualificado (FQDN).

Por exemplo, a fim assinar os Certificados HTTP e XMPP para um único CUCM IM e o nó da presença, você pôde precisar de submeter cada CSR ao público diferente CA.

Verifique se um certificado Auto-é assinado ou CA-assinado

> Nota: Este exemplo é para a versão 8.x CUCM. O processo pôde variar entre server.

1. Navegue a **Cisco unificou a administração do OS**.
2. Escolha o **> gerenciamento de certificado da Segurança**.
3. Encontre e clique o arquivo do **.pem do certificado da Tomcat-confiança**.
4. Clique a **transferência**, e **salvar**.
5. Navegue ao arquivo, e rebatize-o com a extensão de **.cer**.
6. Abra e veja este arquivo (usuários de MS Windows).
7. Verifique **emitido pelo** campo. Se combina **emitido** para colocar, a seguir o certificado Auto-está assinado (veja o **exemplo**).

Exemplo: Auto-assinado contra o certificado assinado CA privado

Privado Auto-assinado CA-assinado

Gerencia um CSR

> Nota: Este exemplo é para a versão 8.x CUCM. O processo pôde variar entre server.

1. Navegue a **Cisco unificou a administração do OS**.
2. Escolha o **> gerenciamento de certificado da Segurança**.
3. O clique **gerencie o CSR**, e escolhe **Tomcat da** lista de drop-down.
4. O clique **gerencie o CSR**, e clica-o **perto**.
5. Clique a **transferência CSR**, e escolha **Tomcat da** lista de drop-down.
6. Clique a **transferência CSR**, e salvar o arquivo.
7. Envie o arquivo **.csr** a ser assinado por seu server privado de CA ou por CA público.
   Nota: Uma vez que você tem este arquivo CSR, o processo varia baseado em seu ambiente.
8. Clique o **certificado/certificate chain da transferência de arquivo pela rede** sob a re-transferência de arquivo pela rede do **> gerenciamento de certificado da Segurança os** certificados assinados novos que foram emitidos a seu server.

Como fazem os certificados de importação I em lojas do certificado do dispositivo de usuário?

Cada certificado de servidor deve ter um certificado de raiz associado atual na loja da confiança no dispositivo de usuário. Cisco Jabber valida os Certificados que os server atuais contra os certificados de raiz na confiança armazenam.

Certificados de raiz de importação na loja do certificado de MS Windows se:

- Os Certificados são assinados por CA que já não existe na loja da confiança, tal como um CA privado em caso afirmativo, você deve importar o certificado de CA privado à loja das Autoridades de certificação de raiz confiável.
- Os Certificados auto-são assinados. Em caso afirmativo, você deve importar certificados auto-assinados à loja da confiança da empresa.

Você pode usar todos os certificados de importação apropriados do método na loja do certificado de MS Windows, como:

- Use os certificados de importação do assistente da importação do certificado individualmente.
- Distribua Certificados aos usuários com a ferramenta da linha de comando CertMgr.exe no server de MS Windows. (Esta opção o exige usar a ferramenta do gerenciador certificado, CertMgr.exe, não o console de gerenciamento dos Certificados MS, CertMgr.msc.)
- Distribua Certificados aos usuários com um GPO no server de MS Windows.

  Nota: Para instruções detalhadas em como aos certificados de importação, refira a documentação apropriada MS.

Identidade do server nos Certificados

Como parte do processo de assinatura, CA especifica a identidade do server no certificado. Quando o cliente valida esse certificado, verifica aquele:

- Uma autoridade confiada emitiu o certificado.
- A identidade do server que apresenta o certificado combina a identidade do server especificada no certificado.

  Nota: O público CA exige geralmente um FQDN como a identidade do server, não um endereço IP de Um ou Mais Servidores Cisco ICM NT.

Campos do identificador

O cliente verifica estes campos do identificador nos certificados de servidor para ver se há um fósforo da identidade:

Certificados XMPP

- SubjectAltName \ OtherName \ xmppAddr
- SubjectAltName \ OtherName \ srvName
- SubjectAltName \ dnsNames
- CN sujeito

Certificados HTTP

- SubjectAltName \ dnsNames
- CN sujeito

  Nota: O campo sujeito do CN pode conter um convite (*) como o caráter leftmost; por exemplo, *.cisco.com. Seus CUCM, COPO, e server do Cisco Unity Connection não puderam apoiar Certificados do convite. (Refira a identificação de bug Cisco CSCta14114 do realce).

Impeça a má combinação da identidade

Quando um cliente do Jabber tenta conectar a um server com um endereço IP de Um ou Mais Servidores Cisco ICM NT, e o certificado de servidor identifica o server com um FQDN, o cliente não pode identificar o server como confiado e alerta o usuário. Assim, se seus certificados de servidor identificam os server com FQDNs, você deve especificar o nome do servidor como o FQDN em muitos lugares em seus server.

A tabela 3 alista todos os lugares que precisam de especificar o nome do servidor enquanto aparece no certificado, se é um endereço IP de Um ou Mais Servidores Cisco ICM NT ou um FQDN.

Tabela 3

Servidor	Lugar (o ajuste deve combinar o certificado)
Cisco Jabber clientes	Endereço do servidor do início de uma sessão (difere para clientes, normalme sob **configurações de conexão)** ** Todos os nomes de nó (**sistema > topologia de cluster)** ** **Cuidado**: Certifique-se de que se você muda este ao FQDN, você pode res este através do DNS ou os server permanecem no estado começando! Servidores TFTP (**aplicativo > Jabber > ajustes de Cisco)** Cisco IP Phone preliminar e secundário do Cisco Call Manager (CCMCIP) **(aplicativo > Jabber de Cisco > perfil CCMCIP)**
COPO (versão 8.x e anterior)	Nome de host do correio de voz (**aplicativo > Jabber > servidor de correio de de Cisco)** Nome do armazenador de mensagens **(aplicativo > Jabber > armazenador de mensagens de Cisco)** Nome de host das Conferências (**aplicativo > de Jabber > de Conferências de Cisco server)** (local de encontro somente) Domínio XMPP (veja o **domínio do fornecimento XMPP à** seção dos **clientes**)
CUCM IM e presença (versão 9.x e mais recente)	** Todos os nomes de nó **(sistema > topologia de cluster**) ** **Cuidado**: Certifique-se de que se você muda este ao FQDN, você pode res este através do DNS ou os server permanecem no estado começando! Servidores TFTP (**aplicativo > clientes > ajustes do legado)** CCMCIP preliminar e secundário **(aplicativo > clientes do legado > perfil CCM** Domínio XMPP (veja o **domínio do fornecimento XMPP à** seção dos **clientes**)
CUCM (versão 8.x e anterior)	Nome do servidor (**sistema > servidor)**
CUCM (versão 9.x e mais recente)	Nome do servidor **(sistema > servidor)** IM e server da presença (**gerenciamento de usuário > configurações de usuá serviço UC > IM e presença)**

	Nome de host do correio de voz **(gerenciamento de usuário > configurações d usuário > serviço > correio de voz UC)** Nome do armazenador de mensagens **(gerenciamento de usuário > configura de usuário > serviço > armazenador de mensagens UC)** Nome de host das Conferências (**(gerenciamento de usuário > configurações usuário > serviço UC > Conferências)** (local de encontro somente)
Cisco Unity Connection (todas as versões)	**Nenhuma mudança necessária**

Forneça o domínio XMPP aos clientes

O cliente identifica Certificados XMPP com o domínio XMPP, um pouco do que com o FQDN. Os Certificados XMPP devem conter o domínio XMPP em um campo do identificador.

Quando o cliente tenta conectar ao server da presença, o server da presença fornece o domínio XMPP ao cliente. O cliente pode então validar a identidade do server da presença contra o certificado XMPP.

Termine estas etapas a fim assegurar-se de que o server da presença forneça o domínio XMPP ao cliente:

1. Abra a interface de administração para seu server da presença, **Cisco unificou CM IM e interface de administração da presença** ou a **interface de administração do Cisco Unified Presence**.
2. Navegue ao **> segurança > aos ajustes do sistema**.
3. Encontre a seção dos **ajustes do certificado XMPP**.
4. Especifique o domínio de servidor da presença no **Domain Name para o campo de nome da alternativa do assunto do certificado de Server-à-server XMPP**.
5. Verifique o **Domain Name do uso para ver se há a** caixa de verificação **alternativa de nome do assunto do certificado XMPP**.
6. Clique em Salvar.
7. Depois que você salvar esta mudança, você deve regenerar o certificado do **copo-xmpp no** server.
8. Reinicie o **roteador XCP** para que a mudança tome o efeito.

   Cuidado: Um reinício do roteador XCP impacta o serviço.

A validação certificada está agora completa!

Informações Relacionadas

- Cisco Jabber 9.2.5 Release Note
- Cisco Jabber: Validação imperativa TechNote do certificado de servidor
- Suporte Técnico e Documentação - Cisco Systems