Integrar ECE com PCCE na versão 12.0 e superior

Contents

Introdução

Este documento descreve as etapas para integrar o Enterprise Chat and Email (ECE) com o Packaged Contact Center Enterprise (PCCE) nas versões 12.0 e posteriores

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- E-mail e bate-papo corporativo (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- ECE 12.5(1)
- PCCE 12.5(1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O PCCE versão 12.0 introduziu uma nova interface de gerenciamento conhecida como SPOG (Single Pane of Glass, painel único de vidro). Quase todo o gerenciamento da central de contatos e dos aplicativos relacionados é executado agora nessa interface. Para integrar corretamente tanto ECE como PCCE, você deve completar várias etapas que são exclusivas para esta integração. Este documento orienta você durante este processo.

Terminologia

Em todo este documento, estes termos são usados.

- E-mail e bate-papo corporativo (ECE) - A ECE é um produto que permite que solicitações de bate-papo e e-mail sejam encaminhadas para agentes da central de contatos da mesma forma que chamadas de voz.
- SPOG (Single Pane of Glass, único painel de controle) - o SPOG é a forma como a administração do PCCE é feita na versão 12.0 e posterior. O SPOG é uma reescrita completa da ferramenta de administração do CCE que foi usada em versões anteriores à 12.0.
- Autoridade de Certificação (CA) - Uma entidade que emite certificados digitais de acordo com um modelo de infraestrutura de chave pública (PKI).

  Há dois tipos de CAs que você pode encontrar.

  - CA pública - uma CA pública é aquela que tem sua raiz e certificados intermediários incluídos na maioria dos navegadores e sistemas operacionais. Algumas CAs públicas comuns incluem IdenTrust, DigiCert, GoDaddy e GlobalSign.
  - CA privada - Uma CA privada é aquela que existe dentro de uma empresa. Algumas CAs privadas são assinadas por CAs públicas, mas na maioria das vezes elas são

CAs autônomas e os certificados emitidos por elas só são confiáveis para os computadores dessa organização.

Em qualquer um dos dois tipos de CA, há dois tipos de servidores de CA.

  - Servidor CA raiz - O servidor CA raiz assina seu próprio certificado. Na implantação padrão de PKI multicamada, a CA raiz está off-line e inacessível. A CA raiz neste modelo também emite certificados somente para outro servidor de CA conhecido como CA intermediário. Algumas empresas optam por usar apenas uma CA de camada única. Neste modelo, a CA raiz emite certificados destinados a serem usados por uma entidade diferente de outro servidor de CA.
  - Servidor CA Intermediário - O servidor CA intermediário ou emissor emite certificados destinados a serem usados por uma entidade diferente de outro servidor CA.
- Microsoft Management Console (MMC) - Um aplicativo incluído no Microsoft Windows que permite que vários snap-ins sejam carregados. Você pode usar os snap-ins para criar um console personalizado para a administração do servidor. Há muitos snap-ins diferentes incluídos no Windows. Uma pequena lista de exemplos inclui Certificados, Gerenciador de Dispositivos, Gerenciamento de Disco, Visualizador de Eventos e Serviços.
- Balanceador de Carga de Rede (NLB) - Um dispositivo ou aplicativo que apresenta vários recursos físicos aos usuários finais com um nome físico comum. Os NLBs são muito comuns com aplicativos e serviços da Web. Os NLBs podem ser implementados de várias maneiras. Quando usado com ECE, o NLB deve ser configurado de forma a assegurar que as sessões do usuário retornem ao mesmo servidor Web físico de back-end através do uso de inserção de cookie ou um método equivalente. Isso é conhecido como uma sessão difícil com inserção de cookie. Sessão sticky refere-se simplesmente à capacidade de um balanceador de carga de retornar a sessão de um usuário para o mesmo servidor back-end físico para todas as interações.
  - Passagem SSL - A passagem SSL é um método no qual a sessão SSL existe entre o dispositivo do usuário final e o servidor Web físico no qual a sessão do usuário foi atribuída. A passagem SSL não permite a inserção de cookies, pois a sessão HTTP é criptografada fisicamente o tempo todo. A maioria dos NLBs suporta sessão sticky com passagem SSL através do uso de tabelas stick que monitoram a parte serverhello e clienthello da configuração da sessão e armazenam os valores exclusivos em uma tabela. Quando a próxima solicitação que corresponder a esses valores for apresentada ao NLB, a tabela de aderência poderá ser usada para retornar a sessão ao mesmo servidor back-end.
  - Descarregamento de SSL - Quando um NLB é configurado para descarregamento de SSL, existem duas sessões ou túneis de SSL para qualquer sessão de usuário final. A primeira é entre o dispositivo de usuário final e o VIP (IP Virtual) configurado no NLB para o site. O segundo é entre o IP de back-end do NLB e o servidor Web físico onde a sessão do usuário é atribuída. O descarregamento de SSL oferece suporte à inserção de cookies, pois o fluxo HTTP é totalmente descriptografado no NLB, onde cookies HTTP adicionais podem ser inseridos e a inspeção de sessão pode ser executada. O descarregamento de SSL é frequentemente usado quando o aplicativo da Web não exige SSL, mas é feito para segurança. As versões atuais do ECE não dão suporte ao acesso ao aplicativo em uma sessão não SSL.

Etapas de Pré-requisito

Há vários pré-requisitos que devem ser preenchidos antes que você comece a integrar os dois sistemas.

- Nível Mínimo de Patch PCCE
  - Versão 12.0(1) - ES37
  - Versão 12.5(1) - Não há mínimo atual para a funcionalidade básica
- Nível Mínimo de Patch ECE

  Recomenda-se que a ECE execute o Especial de Engenharia (ES) mais recente disponível.

  - Versão 12.0(1) - ES3 + ES3_ET1a
  - Versão 12.5(1) - Não há mínimo atual para a funcionalidade básica
- Itens de configuração

  Certifique-se de associar ECE_Email, ECE_Chat e ECE_Outbound Media Routing Domains (MRDs) à Instância de Aplicativo correta.

  - Para o modelo de implantação do Agente PCCE 2000, a Instância do Aplicativo é Multicanal e é pré-configurada quando o PCCE é implantado.
  - Para o modelo de implantação do Agente PCCE 4000/12000, a Instância do aplicativo pode ser qualquer nome e deve ser criada por quem estiver executando a integração. A prática recomendada é usar a forma {site}_{peripheral_set}_{application_instance}. Se você instalou o PCCE com o nome do site como Principal, o periférico definido como PS1 e a instância do aplicativo como Multicanal, o nome da instância do aplicativo será Main_PS1_Multichannel.

Observação: o nome da Instância do Aplicativo diferencia maiúsculas de minúsculas. Certifique-se de digitar o nome corretamente ao adicionar o servidor Web ECE ao inventário.

Etapas de integração

Todos os pormenores relativos a todas as etapas do presente documento são abordados na documentação relativa ao ECE e ao PCCE, mas não são apresentados numa lista nem no mesmo documento. Consulte os links incluídos no final deste documento para obter mais detalhes.

Etapa 1. Configurar Certificados SSL

Você deve gerar um certificado para ser usado pelo servidor Web ECE. Você pode usar um certificado autoassinado, mas geralmente é mais fácil usar um certificado assinado pela CA. Os certificados autoassinados não são menos seguros que os certificados assinados pela CA, há menos etapas para criar inicialmente o certificado, mas quando o certificado precisar ser substituído, você deve lembrar de carregar o novo certificado para os armazenamentos de chaves

Java em todos os servidores de dados de administração do PCCE. Se você usar um certificado assinado pela CA, precisará apenas fazer o upload da raiz e, se presente, dos certificados intermediários para os armazenamentos de chaves.

Se você tiver vários servidores Web em sua implantação, será necessário revisar essas diretrizes. As etapas específicas necessárias para configurar um balanceador de carga de rede estão fora do escopo deste documento. Entre em contato com o fornecedor do balanceador de carga para obter assistência, se necessário.

- Embora não seja necessário, um balanceador de carga simplifica muito a implementação
- O acesso ao aplicativo ECE em cada servidor Web deve usar SSL independentemente do método de balanceador de carga usado
- O balanceador de carga pode ser configurado como passagem SSL ou descarregamento SSL
- Se a passagem SSL for escolhida:
    - Você deve executar todas as operações de certificado de um servidor
    - Quando o certificado estiver configurado corretamente, você deverá exportá-lo e garantir que a chave privada seja incluída em um arquivo PFX (troca de informações pessoais)
    - Você deve copiar o arquivo PFX para todos os outros servidores Web na implantação e importar o certificado para o IIS
- Se o descarregamento de SSL for escolhido, cada servidor Web poderá ser configurado com seu próprio certificado SSL individual

---

Observação: se você tiver vários servidores Web e escolher a passagem SSL no servidor Web, ou se quiser ter um certificado comum em todos os servidores, deverá escolher um servidor Web no qual executar a etapa 1 e, em seguida, importar o certificado para todos os outros servidores Web.
Se você escolher descarregamento de SSL, deverá executar estas etapas em todos os servidores Web. Você também deve gerar um certificado para usar no balanceador de carga.

Etapa 1.1. Gerar um certificado

Você pode ignorar esta seção se já tiver criado ou obtido um certificado; caso contrário, escolha uma das duas opções.

Opção 1. Usar um certificado autoassinado

1. Navegue até Administração do IIS.
2. Selecione o nome do servidor na árvore Conexões à esquerda.
3. Localize Server Certificates no painel central e clique duas vezes para abri-lo.
4. Selecione Criar certificado autoassinado... no painel Ações à direita.

5. Na janela Criar certificado autoassinado, escolha e insira um nome na caixa Especificar um nome amigável para o certificado:. Esse nome é como o certificado aparece no processo de seleção na próxima etapa principal. Esse nome não precisa corresponder ao nome comum do certificado e não afeta a forma como o certificado aparece para o usuário final.
6. Certifique-se de que Personal esteja selecionado na caixa suspensa Select a certificate store for the new certificate:.
7. Selecione OK para criar o certificado.
8. Continue na próxima etapa principal, Vincular certificado ao site.

Opção 2. Usar um Certificado assinado pela CA

Os certificados assinados pela CA exigem que você gere uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado). O CSR é um arquivo de texto que é enviado para a CA onde ele é assinado e, em seguida, o certificado assinado juntamente com os certificados de CA necessários são retornados e o CSR preenchido. Você pode optar por fazer isso por meio da Administração do IIS ou do Console de Gerenciamento Microsoft (MMC). O método de administração do IIS é muito mais fácil, sem necessidade de conhecimento especial, mas permite apenas configurar os campos incluídos no atributo Subject do certificado e alterar o comprimento do bit. O MMC requer etapas adicionais e que você possua um conhecimento completo de todos os campos necessários em um CSR válido. É altamente recomendável usar o MMC apenas se você tiver uma experiência moderada a especializada com criação e gerenciamento de certificados. Se sua implantação exigir que a ECE seja acessada por mais de um nome totalmente qualificado ou se for necessário alterar qualquer parte do certificado, exceto o assunto e o comprimento do bit, você deverá usar o método MMC.

1. Via Administração do IIS

   Use estas etapas para gerar uma CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado) por meio do Gerenciador do IIS.

   1. Navegue até Administração do IIS.
   2. Selecione o nome do servidor na árvore Conexões à esquerda.
   3. Localize Server Certificates no painel central e clique duas vezes para abri-lo.
   4. Selecione Criar solicitação de certificado... no painel Ações à direita. O assistente Solicitar Certificado é exibido.
   5. Na página Propriedades do Nome Distinto, insira os valores no formulário do sistema. Todos os campos devem ser preenchidos. Selecione Avançar para continuar.
   6. Na página Propriedades do Provedor de Serviços de Criptografia, deixe a seleção padrão para Provedor de serviços de Criptografia:. Altere o menu suspenso Bit length: para um mínimo de 2048. Selecione Avançar para continuar.
   7. Na página Nome do arquivo, selecione o local onde deseja salvar o arquivo CSR.
   8. Forneça o arquivo à autoridade de certificação. Depois de receber o certificado assinado, copie-o para o servidor Web e continue com a próxima etapa.
   9. No mesmo local no Gerenciador do IIS, selecione Concluir Solicitação de Certificado no painel Ações. O assistente é exibido.
   10. Na página Specify Certificate Authority Response, escolha o certificado fornecido pela

sua CA. Dê um nome na caixa Nome amigável. Esse nome é como o certificado aparece no processo de seleção na próxima etapa principal. Certifique-se de que a lista suspensa Select a certificate store for the new certificate: esteja definida como Personal.

11. Selecione OK para concluir o upload do certificado.
12. Continue na próxima etapa principal, Vincular certificado ao site.

2. Via Console de Gerenciamento Microsoft (MMC)

Use estas etapas para gerar um CSR por meio do MMC. Esse método permite personalizar cada aspecto do CSR.

1. Clique com o botão direito no botão Iniciar e selecione Executar.
2. Digite mmc na caixa de execução e selecione OK.
3. Adicione o snap-in Certificado à janela do MMC.
    1. Selecione Arquivo e Adicionar/Remover Snap-in.... A caixa Add or Remove Snap-ins é exibida.
    2. Na lista à esquerda, localize Certificates e selecione Add >. A caixa de snap-in Certificados é exibida.
    3. Selecione a opção Conta do computador e, em seguida, selecione Avançar >.
    4. Verifique se Computador local: (o computador em que este console está) está selecionado na página Selecionar computador e selecione Concluir.
    5. Selecione OK para fechar a caixa Adicionar ou remover snap-ins.
4. Gerar o CSR
    1. No painel esquerdo, expanda Certificados (Computador local), depois Pessoal e selecione a pasta Certificados.
    2. Clique com o botão direito do mouse na pasta Certificados e navegue para Todas as Tarefas > Operações Avançadas > e selecione Criar Solicitação Personalizada.... O assistente Inscrição de Certificado é exibido.
    3. Selecione Avançar na tela de introdução.
    4. Na página Selecionar Diretiva de Registro de Certificado, selecione Continuar sem diretiva de registro, listado em Solicitação Personalizada, e selecione Avançar.
    5. Na página Solicitação personalizada, certifique-se de que o Modelo selecionado seja (Nenhum modelo) Chave CNG e que o formato de solicitação seja apropriado para sua CA. O PKCS nº 10 funciona com a CA da Microsoft. Selecione Avançar para prosseguir para a próxima página.
    6. Na página Informações do certificado, selecione a lista suspensa ao lado da palavra Detalhes e, em seguida, selecione o botão Propriedades. O formulário Propriedades do certificado é exibido.
    7. Está além do escopo deste documento fornecer todas as opções para o formulário Propriedades do certificado. Consulte a documentação da Microsoft para obter detalhes. Aqui estão algumas observações e dicas sobre este formulário.
        - Certifique-se de preencher todos os valores necessários na seção Nome do assunto: da guia Assunto:
        - Certifique-se de que o valor fornecido para Nome comum também seja

fornecido na seção Nome alternativo:
    - Defina Type: como DNS, digite o URL na caixa Value: e selecione o botão Add >
    - Se desejar usar vários URLs para acessar o ECE, forneça cada nome alternativo nesse mesmo campo e selecione Add > após cada
    - Certifique-se de definir o tamanho Key na guia Private Key para um valor maior que 1024.
    - Se você planeja exportar o certificado para usar em vários servidores Web, como é feito frequentemente em uma instalação HA, certifique-se de selecionar Tornar a chave privada exportável. Se isso não for feito, não será possível exportar o certificado posteriormente
    - Os valores inseridos e as seleções feitas não são validados. Você deve garantir que você forneça todas as informações necessárias ou que a CA não possa concluir o CSR
8. Depois de selecionar todas as seleções, OK para retornar ao assistente. Selecione Avançar para prosseguir para a próxima página.
9. Na página Onde deseja salvar a solicitação offline?, selecione um nome de arquivo em um local que você possa acessar. Para a maioria das CAs, você deve selecionar Base 64 como o formato.
10. Forneça o arquivo à sua autoridade de certificação. Depois de assiná-lo e devolver o certificado para você, copie o certificado para o servidor Web e continue com as últimas etapas.
11. No snap-in de gerenciamento de certificados do MMC, navegue para Certificados (Computador Local) > Pessoal, clique com o botão direito do mouse em Certificados e escolha Todas as Tarefas > Importar.... O Assistente de Importação de Certificado é exibido.
12. Selecione Next na tela introdutória.
13. Na tela File to import, selecione o certificado que foi assinado por sua CA e selecione Next.
14. Certifique-se de selecionar Place all certificates in the following store.
15. Certifique-se de que Personal esteja selecionado na caixa Certificate store: e selecione Next.
16. Revise a tela final e selecione Finish para concluir a importação.
17. Feche o console MMC. Se for solicitado que você salve as configurações do console, selecione Não. Isso não afeta a importação do certificado.
18. Continue na próxima etapa principal, Vincular certificado ao site.

Etapa 1.2. Vincular Certificado ao Site

⚠ Cuidado: Você deve garantir que o campo de nome do host seja deixado em branco e que a opção Exigir indicação de nome de servidor não seja selecionada na caixa Editar ligação de site. Se qualquer um deles estiver configurado, o SPOG falhará quando tentar se comunicar com o ECE.

---

1. Abra o Gerenciador dos Serviços de Informações da Internet (IIS) se ainda não tiver feito

isso.

2. No painel Conexões à esquerda, navegue para Sites e selecione Site padrão.

   Certifique-se de selecionar o nome correto do site se optar por usar um nome de site diferente do Default Web Site.

3. Selecione Vinculações... no painel Ações à direita. A caixa Ligações de site é exibida.
    1. Se não houver uma linha com Type, https e Port, 443, faça o seguinte. Caso contrário, vá para a próxima etapa principal.
        1. Selecione o botão Add..., a caixa Add Site Binding é exibida.
        2. Selecione https na lista suspensa Tipo:.
        3. Verifique se a lista suspensa IP address: mostra All Unassigned e se o campo Port: é 443.
        4. Certifique-se de deixar o campo Host name: em branco e a opção Require Server Name Indication desmarcada.
        5. No menu suspenso SSL certificate:, selecione o nome do certificado que corresponde ao que você criou anteriormente.
            - Se você não tiver certeza de qual certificado escolher, use o botão Selecionar... para exibir e pesquisar os certificados presentes no servidor
            - Use o botão View... para exibir o certificado escolhido e verificar se os detalhes estão corretos
        6. Selecione OK para salvar sua seleção.
    2. Selecione a linha que mostra https na coluna Tipo e, em seguida, selecione o botão Editar.... A caixa de diálogo Editar vinculação de site é exibida.
        1. Verifique se a lista suspensa IP address: mostra All Unassigned e se o campo Port: é 443.
        2. Verifique se o campo Host name: foi deixado em branco e se a opção Require Server Name Indication não está selecionada.
        3. No menu suspenso SSL certificate:, selecione o nome do certificado que corresponde ao que você criou anteriormente.
            - Se você não tiver certeza de qual certificado escolher, use o botão Selecionar... para exibir e pesquisar os certificados presentes no servidor
            - Use o botão View... para exibir o certificado escolhido e verificar se os detalhes estão corretos
        4. Selecione OK para salvar sua seleção.
    3. Selecione Fechar para retornar ao Gerenciador do IIS.
4. Feche o Gerenciador do IIS.

Etapa 2. Configurar SSO do Administrador de Partição

A configuração SSO do administrador de partição permite que a ECE crie automaticamente uma conta de usuário de nível de partição para qualquer administrador que abra o gadget ECE no SPOG.

Observação: você deve configurar o SSO do Administrador de Partição mesmo que não planeje ativar o SSO do Agente ou Supervisor.

Etapa 2.1. Obtenha o certificado do Ative Diretory (AD) e crie o armazenamento de chaves.

Esta etapa pode ser necessária para lidar com as recentes alterações de segurança anunciadas pela Microsoft. Se a atualização não for aplicada e as alterações não forem feitas no domínio, isso poderá ser ignorado.

Para obter detalhes, consulte Microsoft KB4520412 details.

1. Obtenha o certificado SSL, no formato Base 64, no servidor do AD fornecido no formulário Configuração do Administrador de Partição. Um método é mostrado.
    1. Use uma estação de trabalho para baixar e instalar uma cópia do OpenSSL para Windows de, OpenSSL. A edição Light é adequada.
    2. Inicie o prompt de comando do OpenSSL.
    3. Execute este comando. Substitua o nome do servidor pelo nome totalmente qualificado do controlador de domínio do Catálogo Global.
       openssl s_client -connect gcdcsrv01.example.local:3269
    4. Na saída, localize a linha de certificado do servidor.

```
C:openssl s_client -connect 14.10.162.6:3269
CONNECTED(00000003)
depth=1 DC = com, DC = massivedynamic, CN = MassiveDynamic Enterprise CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:
   i:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
 1 s:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
   i:/C=US/OU=pki.uclabservices.com/O=Cisco Systems Inc/CN=UCLAB Services Root
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIH1DCCBbygAwIBAgITJwAAAAbAAn/HKFuWCQAAAAAABjANBgkqhkiG9w0BAQsF
ADBcMRMwEQYKCZImiZPyLGQBGRYDY29tMR4wHAYKCZImiZPyLGQBGRYObWFzc2l2
ZWR5bmFtaWMxJTAjBgNVBAMTHE1hc3NpdmVEeW5hbWljIEVudGVycHJpc2UgQ0Ew
HhcNMjAwNDE1MDAxNDM0WhcNMjEwNDE1MDAxNDM0WjAAMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxFajhqjrWqQHfqTXg+SXP5pzvNVrTHIigrAam8D0
```

    5. Copie a saída do início de "-----BEGIN CERTIFICATE-----" até "-----END CERTIFICATE-----". Certifique-se de que as linhas BEGIN CERTIFICATE e END CERTIFICATE estejam incluídas.
    6. Cole as informações copiadas em um novo arquivo de texto e salve-as no computador com uma extensão crt.
2. Copie o arquivo de certificado para um dos servidores de aplicativos.
3. Abra uma sessão RDP no servidor do aplicativo no qual você copiou o certificado.
4. Crie um novo armazenamento de chaves Java.
    1. Abra um prompt de comando no Servidor de Aplicativos.
    2. Mude para o diretório bin do ECE Java Development Kit (JDK).
    3. Execute este comando. Substitua os valores conforme apropriado.
       keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword

5. Nas versões anteriores à 12.6, copie o armazenamento de chaves para o mesmo caminho em todos os outros servidores de aplicativos em seu ambiente. Com a versão 12.6, copie o armazenamento de chaves em um local acessível a partir da estação de trabalho onde você configura a ECE.

Etapa 2.2. Configure ECE com Informações de Acesso ao Lightweight Diretory Access Protocol (LDAP) AD.

1. Em uma estação de trabalho ou computador com o Internet Explorer 11, navegue até a URL da partição Comercial.

 Dica: a partição Comercial também é conhecida como Partição 1. Para a maioria das instalações, a partição Comercial pode ser acessada por meio de uma URL semelhante a https://ece.example.com/default.

---

2. Faça login como pa e forneça a senha para o seu sistema.
3. Depois de fazer login com êxito, selecione o link Administration no console inicial.
4. Navegue até a pasta Configuração de SSO, Administração > Partição: padrão > Segurança > SSO e Provisionamento.
5. No painel superior à direita, selecione a entrada Partition Administration Configuration.
6. No painel inferior à direita, insira os valores para o Lightweight Diretory Access Protocol (LDAP) e o AD.
    1. URL LDAP - Como prática recomendada, use o nome de um Controlador de Domínio do Global Catalog (GC).
    Se você não usar um GC, poderá ver um erro nos logs do ApplicationServer da seguinte maneira.
    Exceção na autenticação LDAP <@>
    javax.naming.PartialResultException: Referência(s) de continuidade não processada(s); nome restante 'DC=example,DC=com'
        - A porta do Catálogo Global não segura é 3268
        - A porta do catálogo global seguro é 3269
    2. Atributo DN - Deve ser userPrincipalName.
    3. Base - Isso não é necessário se você usar um GC, caso contrário, você deve fornecer o formato LDAP apropriado de base.
    4. DN para pesquisa LDAP - a menos que o seu domínio permita a associação anônima, você deve fornecer o nome distinto de um usuário com a capacidade de vincular ao LDAP e pesquisar a árvore de diretórios.

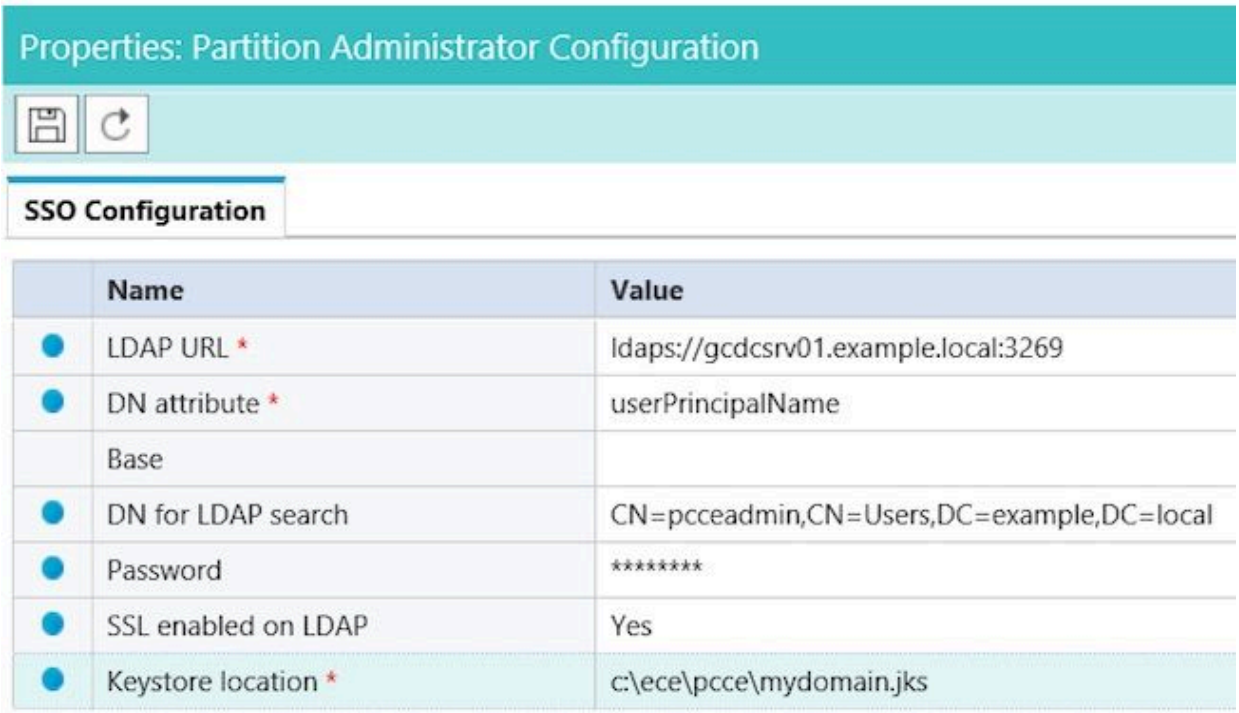
     Dica: a maneira mais fácil de encontrar o valor correto para o usuário é usar a ferramenta Usuários e Computadores do Ative Diretory. Essas etapas mostram como localizar esse valor.

    ---

        1. No menu Exibir, selecione a opção Recursos avançados.
        2. Navegue até o objeto do usuário, clique com o botão direito do mouse e escolha Propriedades.
        3. Selecione a guia Atributos.

4. Selecione o botão Filtro e, em seguida, selecione Mostrar apenas atributos com valores.
5. Localize distinquishedName na lista e clique duas vezes para exibir o valor.
6. Realce o valor mostrado e, em seguida, copie-o e cole-o em um editor de texto.
7. Copie e cole o valor do arquivo de texto no campo DN para pesquisa LDAP. O valor deve ser semelhante a, CN=pcceadmin, CN=Users, DC=example, DC=local

5. Senha - Forneça a senha para o usuário especificado.
6. SSL ativado no LDAP - Esse campo pode ser considerado obrigatório para a maioria dos clientes.
7. Local do armazenamento de chaves - Deve ser o local do armazenamento de chaves no qual você importou o certificado SSL do AD. No exemplo, é c:\ece\pcce\mydomain.jks, como mostrado na imagem:



7. Selecione o ícone do disquete para salvar as alterações.

Etapa 3. Validar arquivo de configuração

A conclusão desta seção é obrigatória para todas as instalações da versão 12.0. Para qualquer versão diferente da 12.0, você poderá ignorar esta seção.
Há dois cenários adicionais com todas as versões em que essa etapa pode ser necessária. A primeira é quando o ECE foi instalado em uma configuração de alta disponibilidade. O segundo, e mais comum, é quando o nome do host do servidor Web não corresponde ao nome que você usa para acessar ECE. Por exemplo, se você instalar o servidor Web ECE em um servidor com o nome de host UCSVRECEWEB.example.com, mas os usuários acessarem as páginas Web ECE com o URL chat.example.com, esta seção deverá ser concluída. Se o nome de host do servidor e o URL com o qual você acessa o ECE forem os mesmos e se você tiver instalado a versão 12.5 ou superior, você pode pular esta etapa e concluir a seção.

Substitua {ECE_HOME} pelo local físico onde você instalou o ECE. Por exemplo, se você instalou ECE em C:\Cisco, substitua {ECE_HOME} por C:\Cisco em cada local.

Dica: use um editor de texto como o Notepad++ em vez do Notepad ou do Wordpad, pois eles não interpretam as terminações de linha corretamente.

---

1. Abra uma sessão de área de trabalho remota para todos os servidores web ECE em sua implantação.
2. Navegue até este caminho, {ECE_HOME}\eService\templates\finesse\gadget\spog.
3. Localize o arquivo spog_config.jsfile e faça uma cópia de backup em um local seguro.
4. Abra o arquivo spog_config.jsatual em um editor de texto.
5. Localize essas duas linhas e atualize-as para que correspondam à sua implantação.
   O web_server_protocol deve ser https, atualize se necessário.
   Atualize o web_server_name para corresponder ao nome totalmente qualificado que você alocou para usar para acessar o ECE. Exemplo: ece.example.com
   - var web_server_protocol = "https";
   - var web_server_name = "ece.example.com";
6. Salve as alterações.
7. Repita o procedimento em todos os outros servidores da Web em sua implantação.

Etapa 4. Adicionar ECE ao inventário PCCE

A partir da versão 12.0, o PCCE tem 3 opções de implantação diferentes: 2000 Agent (2K Agent), 4000 Agent (4K Agent) e 12000 Agent (12K Agent). Essas três opções de implantação podem ser separadas em dois grupos, Agente 2K e Agente 4K/12K. Eles são separados dessa maneira, pois há várias diferenças fundamentais em como eles parecem no SPOG. A seguir a este parágrafo, procede-se a uma comparação muito aprofundada dos dois métodos. Este documento não fornece etapas específicas para adicionar um componente ao inventário. Consulte os links no final deste documento para obter detalhes específicos sobre este processo. Esta seção aborda detalhes específicos que devem ser verificados quando você adiciona ECE ao PCCE. Este documento também pressupõe que a instalação do PCCE foi concluída e que você pode acessar e configurar outros aspectos da solução.

- Implantação de agente de 2K
  - A configuração inicial dos componentes do PCCE é feita inteiramente por meio da Administração do CCE e é automatizada
  - Novos componentes são adicionados na página Inventário através de uma caixa pop-up onde você insere os detalhes, como o IP ou o nome do host e quaisquer credenciais necessárias ou configuração específica do componente
- Implantação de agentes de 4K e 12K
  - Grande parte da configuração inicial reflete as etapas usadas para UCCE
  - Os componentes são adicionados por meio de um arquivo CSV (Comma-Separated Values, valores separados por vírgula) que você baixa da Administração do CCE, preenche conforme sua instalação específica e carrega
  - A implantação inicial requer que alguns componentes específicos sejam incluídos no primeiro arquivo CSV

- Os componentes que não foram adicionados quando o sistema foi configurado inicialmente são adicionados por meio de arquivos CSV que contêm as informações necessárias

Etapa 4.1. Carregar o certificado do servidor Web ECE no armazenamento de chaves Java

1. Se os certificados autoassinados forem usados
    1. Abra uma conexão de área de trabalho remota com o Servidor de Dados de Administração (ADS) principal do lado A.
    2. Abra o Internet Explorer 11 como administrador e navegue até a partição comercial ECE.
    3. Selecione o ícone de um cadeado no lado direito da barra de URL e, em seguida, selecione View Certificates.
    4. Na caixa Certificado, selecione a guia Detalhes.
    5. Selecione Copiar para arquivo... próximo à parte inferior da guia.
    6. No Assistente de Exportação de Certificado, selecione Próximo até chegar à página Formato do Arquivo de Exportação. Certifique-se de selecionar o formato X.509 codificado na base 64 (.CER).
    7. Salve o certificado em um local como c:\Temp\certificates no servidor ADS para concluir a exportação.
    8. Copie o certificado para todos os outros servidores ADS.
    9. Abra um prompt de comando administrativo.
    10. Vá para o diretório inicial Java e, em seguida, para o diretório bin. O diretório inicial do Java pode ser acessado com o seguinte. cd %JAVA_HOME%\bin
    11. Faça backup do arquivo cacerts atual. Copie o arquivo cacerts de %JAVA_HOME%\lib\security para outro local.
    12. Execute este comando para importar o certificado que você salvou anteriormente. Se a senha do armazenamento de chaves não for 'changeit', atualize o comando para corresponder à sua instalação.
        keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN do servidor ECE> -file <Local onde você salvou o certificado>
    13. Reinicie o servidor ADS.
    14. Repita as etapas de 8 a 12 nos outros servidores ADS.
2. Se os certificados assinados por CA forem usados
    1. Obtenha o certificado raiz e intermediário no formato DER/PEM e copie-os para um local como C:\Temp\certificates em todos os servidores ADS.

        Observação: entre em contato com o administrador da CA para obter esses certificados.

        ---

    2. Abra uma conexão de área de trabalho remota com o ADS do lado A principal.
    3. Abra um prompt de comando administrativo.
    4. Vá para o diretório inicial Java e, em seguida, para o diretório bin. O diretório inicial do Java pode ser acessado com o seguinte. cd %JAVA_HOME%\bin
    5. Faça backup do arquivo cacerts atual. Copie o arquivo cacerts de %JAVA_HOME%\lib\security para outro local.

6. Execute este comando para importar o certificado que você salvou anteriormente. Se a senha do armazenamento de chaves não for 'changeit', atualize o comando para corresponder à sua instalação.
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias **<**Nome da raiz de CA**>** -file **<**Local onde você salvou o certificado raiz**>**
7. Repita a Etapa 6 e importe o certificado intermediário, se houver.
8. Reinicie o servidor ADS.
9. Repita as etapas 2 a 12 em todos os outros servidores ADS.

Etapa 4.2. Adicionar o servidor de dados ECE ao inventário

- Embora o servidor de dados deva existir no inventário do sistema, nenhuma comunicação direta é feita entre o PCCE ADS e o servidor de dados
- Quando o ECE é implantado na implantação de 1.500 agentes, o servidor de dados é o servidor de serviços
- Quando o ECE for instalado em uma configuração de alta disponibilidade, adicione apenas o servidor de serviços do lado A

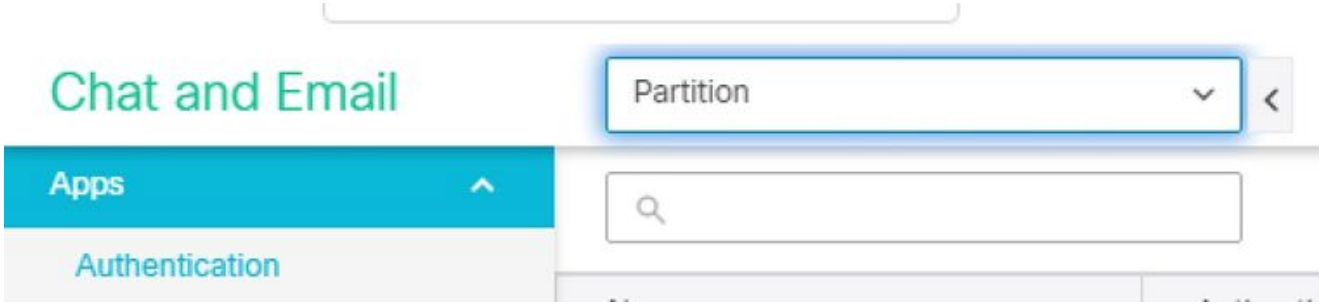
Etapa 4.3. Adicionar o servidor Web ECE ao inventário

- Certifique-se de adicionar o servidor Web com o nome totalmente qualificado
  - Esse nome deve corresponder ao nome comum no certificado ECE ou deve ser listado como um dos nomes alternativos do assunto (SAN)
  - Você não deve usar apenas o nome do host ou o endereço IP
- O nome de usuário e a senha para ECE devem ser as credenciais de logon do pa
- Verifique se a Instância do Aplicativo está correta
  - O nome da Instância do Aplicativo diferencia maiúsculas de minúsculas
  - Para as implantações do 2000 Agent PCCE, a instância do aplicativo é MultiChannel
  - Para as implantações do PCCE do agente 4000/12000, a instância do aplicativo contém o conjunto de site e periférico como parte do nome
- Quando o ECE é instalado com mais de um servidor Web, por exemplo, na implantação do 1500 Agent ou em uma implantação do 400 Agent HA, você pode usar a URL que aponta para o balanceador de carga ou a URL que aponta para cada servidor Web individual como o nome totalmente qualificado do servidor Web. A prática recomendada é usar um balanceador de carga.
- Se você tiver mais de uma implantação ECE, ou se você optar por adicionar cada servidor Web individual na implantação com mais de um, você deve escolher o servidor Web correto ao abrir o gadget ECE no SPOG.

Etapa 5. Integrar ECE com PCCE

1. Faça login na Administração do CCE como administrador.
2. Selecione o cartão Email and Chat e, em seguida, o link Email and Chat como mostrado na imagem.

3. Revise o servidor atualmente selecionado no menu suspenso Nome do dispositivo. Se você adicionou ambos os servidores da Web em uma instalação de alta disponibilidade, poderá escolher qualquer um deles. Se você adicionar uma segunda implantação ECE ao seu sistema posteriormente, certifique-se de selecionar o servidor apropriado antes de continuar.
4. Na lista suspensa ao lado de Bate-papo e E-mail, selecione Partição ou Global como mostrado na imagem.



5. No menu superior, selecione Integration, depois selecione a seta ao lado de Unified CCE e selecione o segundo Unified CCE como mostrado na imagem.

6. Preencha os valores na guia Detalhes AWDB para sua instalação e selecione o botão Salvar.
7. Selecione a guia Configuração e complete-a da seguinte maneira.
    1. Selecione a lista suspensa ao lado de Application Instance e selecione a Application Instance criada para ECE.

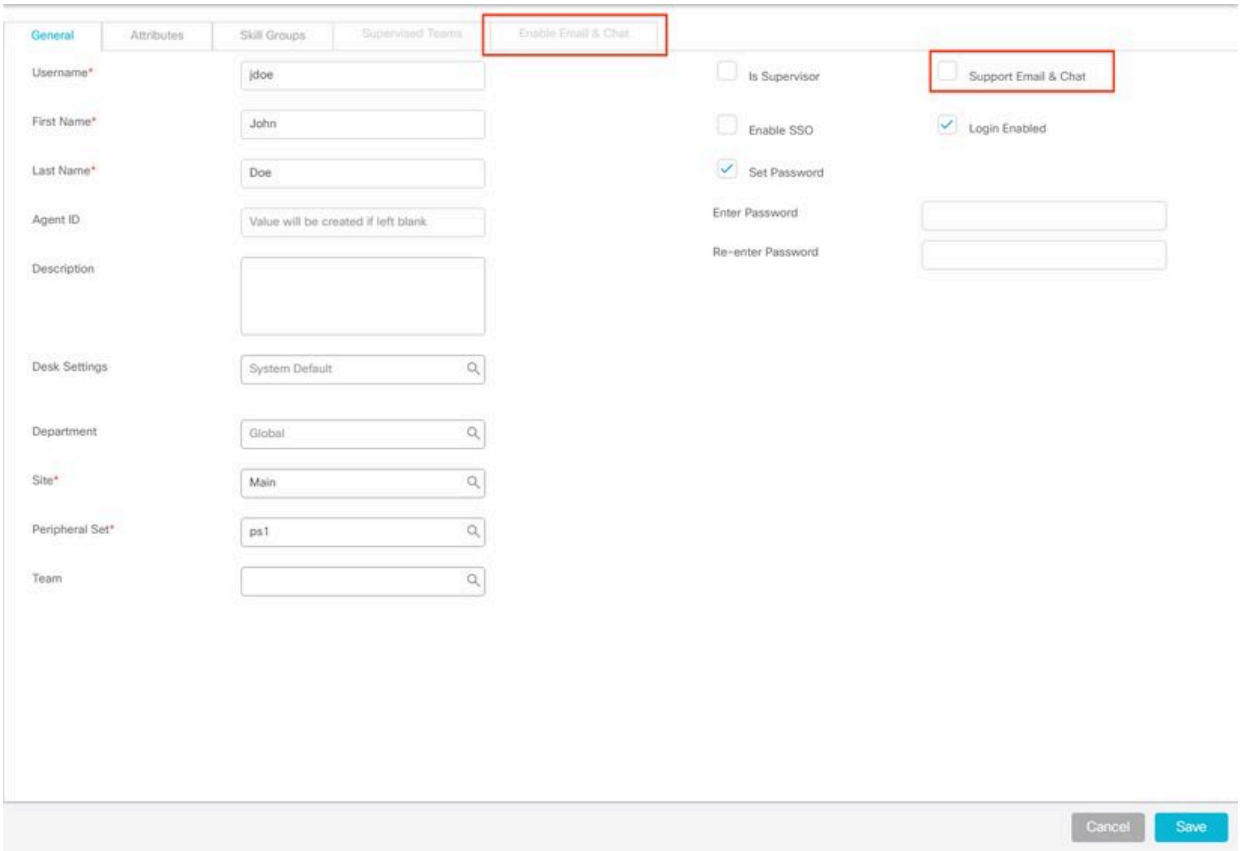
> Observação: esta não deve ser a Instância do Aplicativo que começa com UQ.

    2. Selecione o círculo verde com o botão de sinal de adição branco e selecione o PG do agente.
        1. Selecione o PG do agente (ou PGs do agente, se houver mais de um).
        2. Selecione Salvar depois de adicionar todos os PGs do agente.

> Aviso: depois que você selecionar Salvar, o sistema será permanentemente conectado ao PCCE e não poderá ser desfeito. Se ocorrerem erros nesta seção, você deve desinstalar completamente o ECE e descartar todos os bancos de dados e, em seguida, instalar o ECE como se fosse uma instalação nova.

Etapa 6. Validar Integração ECE

1. Na Administração do CCE, verifique se não há alertas mostrados na barra de status superior. Se houver alertas, selecione a palavra Alerts e revise a página Inventory para garantir que nenhum dos alertas seja para os servidores ECE.
2. Selecione Usuários e, em seguida, Agentes na barra de navegação à esquerda.
3. Selecione um agente na lista e verifique isso.
    1. Agora você verá uma nova caixa de seleção para E-mail e bate-papo de suporte na guia Geral.
    2. Agora você verá uma nova guia chamada Habilitar email e bate-papo como mostrado na imagem.



4. Habilitar um agente de teste para ECE.
    1. Marque a caixa de seleção Support Email & Chat e observe que a guia Enable Email & Chat agora pode ser selecionada.
    2. Selecione a guia Enable Email & Chat e forneça um valor no campo Screen Name.
    3. Selecione Save para atualizar o usuário.
    4. Você recebe uma mensagem de êxito.
5. Verifique se a ECE foi atualizada.

1. Selecione o botão de navegação Visão geral e, em seguida, selecione o cartão e o link E-mail e bate-papo.
2. Na lista suspensa ao lado de Bate-papo e E-mail, selecione o nome que corresponde ao departamento do agente.

Observação: o departamento Serviço no ECE contém todos os objetos que pertencem ao departamento Global no PCCE. O nome do departamento Serviço é, portanto, um valor reservado.

---

1. No menu superior, selecione User Management e, em seguida, selecione Users no menu em Chat and Email.
2. Verifique se você vê o novo agente na lista.

Troubleshooting

É recomendável que você faça o download de várias ferramentas e as mantenha nos servidores ECE. Isso facilita muito a solução de problemas e a manutenção da solução ao longo do tempo.

- Um editor de texto, como o Notepad++
- Uma ferramenta de arquivamento, como o 7-Zip
- Um dos muitos programas do Tail for Windows
  Alguns exemplos são:
  - Cauda descalça
  - Tail para Win32

Para solucionar problemas de integração, você deve primeiro conhecer alguns arquivos de log principais e o local de cada um.

1. Nomes de arquivo e locais no ECE

Há muitos registros no sistema ECE, esses são apenas os mais úteis quando você tenta solucionar um problema de integração.

Arquivo de log	Servidor	Convenção de nomes	Descrição
Servidor do aplicativo	C/A	eg_log_{HOSTNAME}_ApplicationServer.log	Logs do Servidor Wildfly
Atribuição de agente externo	C/S	eg_log_{HOSTNAME}_EAAS-process.log	Interação com MR PG
Mensagens de	C/S	eg_log_{HOSTNAME}_EAMS-process.log	Interação com o servidor CTI

Agente Externo			
Logs raiz	C/A/M/S	egpl_root_{HOSTNAME}.log	Registros entre processos, HazelCast, erros gerais
Status do componente	C/A/M/S	eg_log_{HOSTNAME}_component-status.log	Início do processo e conclusão da cópia do arquivo
Iniciador de processos	C/A/M/S	eg_log_{HOSTNAME}_ProcessLauncher.log	Registros gerais para inicialização de serviço e processo
Gerenciador de serviços distribuídos	C/S	eg_log_{HOSTNAME}_DSMController.log	Logs que mostram o início e a interrupção do processo no servidor de Serviços

Chave do servidor:

- C = Servidor colocado
- A = Servidor de aplicativos
- S = Servidor de serviços
- M = Servidor de mensagens

A maioria dos arquivos de log também tem dois outros logs associados a eles.

- eg_log_{SERVERNAME}_{PROCESS}.log - Log do processo primário
- eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Uso do pool de conexão
- eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Atualizado quando uma consulta falha devido ao tempo limite

2. Nomes de arquivo e locais no PCCE

Os logs do PCCE para problemas de integração estão todos localizados no ADS do lado A. Estes são os registros mais importantes ao solucionar problemas de integração. Cada um deles está localizado em, C:\icm\tomcat\logs.

Arquivo de log	Convenção de nomes	Descrição
CCBU	CCBU.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	Log principal para o CCE Admin e todos os aplicativos da Web relacionados
Erro de	Erro.{YYYY}-{MM}-	Erros vistos pelo administrador do CCE e aplicativos da

CCBU	{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	Web relacionados
Catalina	catalina.{YYYY}-{MM}-{DD}.log	Log nativo do Tomcat, mostra erros de certificado
Tomcat stdout	tomcat9-stdout.{AAAA}-{MM}-{DD}.log	Mensagens de log de saída padrão do Tomcat
Tomcat stderr	tomcat9-stderr.{YYYY}-{MM}-{DD}.log	Mensagens de log de erros padrão do Tomcat

Desses registros, os três primeiros são os solicitados e revisados com mais frequência.

Use estas etapas para definir níveis de rastreamento e coletar os logs necessários.

3. Configuração de Nível de Rastreamento

Este ponto aplica-se apenas à ECE. Os logs necessários do PCCE têm o nível de rastreamento definido pela Cisco e não podem ser alterados.

1. Em uma estação de trabalho ou computador com o Internet Explorer 11, navegue até a URL da partição Sistema.

   Dica: a partição Sistema também é conhecida como Partição 0. Para a maioria das instalações, a partição Sistema pode ser acessada por meio de um URL semelhante a https://ece.example.com/system

2. Efetue login como sa e forneça a senha para seu sistema.
3. Depois de fazer login com êxito, selecione o link System no console inicial.
4. Na página Sistema, expanda Sistema > Recursos compartilhados > Logger > Processos.
5. No painel superior direito, localize o processo para o qual deseja alterar o nível de rastreamento e selecione-o.
   Observação: em um sistema de alta disponibilidade e em um sistema com mais de um servidor de aplicativos, os processos são listados mais de uma vez. Para garantir a captura dos dados, defina o nível de rastreamento para todos os servidores que contêm o processo.
6. No painel inferior direito, selecione a lista suspensa Nível máximo de rastreamento e selecione o valor apropriado.
   Existem 8 níveis de traço definidos na ECE. Os 4 da lista são os usados com mais frequência.
   - 2 - Erro - Nível de rastreamento padrão para processos
   - 4 - Informações - Nível de rastreamento geralmente usado para resolução de problemas
   - 6 - Dbquery - Frequentemente útil para diagnosticar problemas no início da configuração ou problemas mais complexos
   - 7 - Depuração - Saída muito detalhada, necessária apenas nas questões mais complexas

> Observação: não deixe nenhum processo em 6 - Dbquery ou superior por um longo período de tempo e, em geral, apenas com a orientação do TAC.

Mantenha a maioria dos processos no nível de rastreamento, 2-Erro. Se você selecionar o nível 7 ou 8, também deverá selecionar uma duração máxima. Quando o tempo de duração máximo é atingido, o nível de rastreamento retorna ao último nível definido.
Depois que o sistema estiver configurado, altere esses quatro processos para rastrear o nível 4.

- Processo EAAS
- processo EAMS
- dx-process
- processo RX

7. Selecione o ícone salvar para definir o novo nível de rastreamento.

4. Coleção de Arquivos de Log

1. Abra uma Sessão da Área de Trabalho Remota no servidor onde o processo registra o que é necessário.
2. Navegue até o local do arquivo de log.
    1. Servidores ECE

        Os registros são gravados da seguinte forma.

        - Por padrão, os logs são arquivos gravados com tamanho máximo de 5 MB
        - Quando um arquivo de log atinge o máximo configurado, ele é renomeado no formato {LOGNAME}.log.{#}
        - O ECE mantém os 49 arquivos de log anteriores mais o arquivo atual
        - O log atual sempre termina com .log e nenhum número após
        - Os registros não são arquivados nem compactados
        - A maioria dos registros tem uma estrutura comum
        - Os arquivos de log usam **<@>** para separar as seções
        - Os logs são sempre gravados no horário GMT+0000

        Os registros ECE estão localizados em locais diferentes com base na instalação específica.

        1. Implantações de 400 agentes
            1. Frente e verso
                - Servidor: Servidor colocado
                - Local: {ECE_HOME}\eService_RT\logs
            2. Alta disponibilidade
                - Servidores: Ambos os Servidores Colocados
                - Local: {ECE_HOME}\eService\logs

- O diretório criado para o compartilhamento do Sistema de Arquivos Distribuído (DFS) contém apenas logs para instalação e atualizações.
- Somente o servidor que possui a função DSM (Distributed Systems Manager) grava logs para os componentes que fazem parte da Função de Serviços
  - O proprietário da função DSM pode ser encontrado na guia Processos do Gerenciador de Tarefas do Windows. Há de 10 a 15 processos Java neste servidor que não estão no servidor secundário.
  - Os componentes no DSM incluem EAAS, EAMS, Retriever, Dispatcher, Workflow e assim por diante.

2. Implantações de 1.500 agentes
   - Logs localizados no servidor que hospeda a função
   - Local: {ECE_HOME}\eService\logs
   - Com exceção do servidor de serviços, todos os servidores operam e gravam logs para todos os processos associados ao componente
   - Em uma implantação de alta disponibilidade, o servidor de Serviços opera em configuração Ativo/Standby
   - Somente o servidor que possui a função DSM (Distributed Systems Manager) grava logs
   - O proprietário da função DSM pode ser identificado pelo número de processos vistos no Gerenciador de Tarefas do Windows. Há de 10 a 15 processos Java que são executados no servidor primário e apenas 4 processos Java no servidor secundário

2. Servidores PCCE
   - Os registros necessários do PCCE estão localizados em, C:\icm\tomcat\logs
   - Os logs do Tomcat não são sobrepostos ou arquivados
   - Os logs são gravados na hora do servidor local

3. Colete todos os logs que foram criados ou modificados após a observação do problema.
   Uma explicação completa dos logs e dos problemas vistos está além do escopo deste documento. Alguns problemas comuns, o que revisar e algumas soluções possíveis são os seguintes.
   - Problemas relacionados ao certificado
     - Certificado não importado
       - Comportamento: ao tentar abrir o gadget ECE no SPOG, você verá o erro "Erro ao carregar a página. Entre em contato com o administrador."
       - Verifique se há erros semelhantes no log do Catalina no PCCE javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: Falha na criação do caminho PKIX: sun.security.provider.certpath.SunCertPathBuilderException: não foi possível localizar o caminho de certificação válido para o destino

solicitado
        - Resolução: certifique-se de que você importou o Certificado de Servidor Web ECE ou os certificados CA apropriados para o armazenamento de chaves no ADS
    - Incompatibilidade de certificado
        - Comportamento: ao tentar abrir o gadget ECE no SPOG, você verá um erro que indica que o nome comum do certificado ou o nome alternativo do assunto não corresponde ao nome configurado.
        - Verificar: Validar o Certificado SSL
        - Resolução: Certifique-se de que o campo Nome comum no Assunto ou um dos campos DNS no Nome alternativo do assunto contenha o nome totalmente qualificado que você inseriu no SPOG como o nome do servidor Web.
- Problemas do sistema
    - Serviço Não Iniciado
        - Comportamento: ao tentar abrir o gadget ECE no SPOG, você verá o erro "A página da Web em https://{url} pode estar temporariamente inativa ou pode ter sido movida permanentemente para um novo endereço".
        - Verificar: Verifique se o Serviço Windows - Serviço Cisco foi iniciado em todos os servidores ECE, com exceção do servidor Web. Verifique se há erros nos logs raiz no servidor de aplicativos
        - Resolução: Inicie o Cisco Service em todos os serviços ECE.
- Problema de configuração
    - Configuração LDAP
        - Comportamento: ao tentar abrir o gadget ECE no SPOG, você verá o erro "Erro ao carregar a página. Entre em contato com o administrador."
        - Verificar: Aumente o nível de rastreamento do Servidor de Aplicativos para o nível 7 - Depurar, depois tente fazer login novamente e examine o log do Servidor de Aplicativos. Procure a palavra LDAP.
        - Resolução: Valide a configuração LDAP para o Administrador de Partição SSO para garantir que esteja correto.

Informações Relacionadas

Estes são os documentos principais que você deve revisar cuidadosamente antes de iniciar qualquer instalação ou integração ECE. Esta não é uma lista completa de documentos ECE.

⚠ Cuidado: a maioria dos documentos ECE tem duas versões. Certifique-se de fazer o download e usar as versões que são para o PCCE. O título do documento é para o Packaged Contact Center Enterprise ou (para PCCE) ou (para UCCE e PCCE) após o número da versão.

Verifique a página inicial da documentação do Cisco Enterprise Chat and Email para obter

atualizações antes de qualquer instalação, atualização ou integração.

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

- 12.0
  - Guia de instalação e configuração de e-mail e bate-papo corporativo
  - Guia de atualização de e-mail e bate-papo corporativo
  - Guia do administrador de e-mail e bate-papo corporativo
- 12.5
  - Guia de instalação e configuração de e-mail e bate-papo corporativo
  - Guia de atualização de e-mail e bate-papo corporativo
  - Guia do administrador de e-mail e bate-papo corporativo

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.