버전 12.0 이상에서 ECE와 PCCE 통합

목차

소개

이 문서에서는 버전 12.0 이상에서 ECE(Enterprise Chat and Email)를 PCCE(Packaged Contact Center Enterprise)와 통합하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ECE(Enterprise Chat and Email) 12.x

- PCCE(Packaged Contact Center Enterprise) 12.x

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

PCCE 버전 12.0에는 SPOG(Single Pane of Glass)라는 새로운 관리 인터페이스가 도입되었습니다. 이제 컨택 센터 및 관련 애플리케이션의 거의 모든 관리가 이 인터페이스에서 수행됩니다.ECE와 PCCE를 적절하게 통합하려면 이 통합에 고유한 몇 가지 단계를 완료해야 합니다.이 문서는 이 프로세스를 안내합니다.

용어

이 문서에서 이러한 용어가 사용됩니다.

- ECE(Enterprise Chat and Email) - ECE는 음성 통화와 동일한 방식으로 이메일 및 채팅 요청을 컨택 센터 상담원에게 라우팅할 수 있는 제품입니다.
- SPOG(Single Pane of Glass) - SPOG는 PCCE 관리를 버전 12.0 이상에서 수행하는 방법입니다.SPOG는 12.0 이전 버전에서 사용된 CCE 관리 툴의 완전한 재작성입니다.
- CA(Certificate Authority) - PKI(Public Key Infrastructure) 모델에 따라 디지털 인증서를 발급하는 엔티티입니다. 두 가지 유형의 CA가 있을 수 있습니다.퍼블릭 CA - 퍼블릭 CA는 대부분의 브라우저 및 운영 체제에 포함된 루트 및 중간 인증서를 포함하는 CA입니다.일부 공용 CA에는 IdenTrust, DigiCert, GoDaddy 및 GlobalSign 등이 있습니다.프라이빗 CA - 프라이빗 CA는 회사 내에 있는 CA입니다.일부 프라이빗 CA는 공용 CA에서 서명하지만, 대부분의 경우 독립형 CA와 해당 조직의 컴퓨터에서만 신뢰하는 인증서를 발급합니다.두 CA 유형 중 하나에 두 가지 유형의 CA 서버가 있습니다.루트 CA 서버 - 루트 CA 서버는 자체 인증서를 서명합니다.표준 멀티티어 PKI 구축에서 루트 CA는 오프라인 상태이며 액세스할 수 없습니다.이 모델의 루트 CA는 중간 CA라고 하는 다른 CA 서버에만 인증서를 발급합니다.일부 기업은 단일 계층 CA만 사용하도록 선택합니다.이 모델에서는 루트 CA가 다른 CA 서버가 아닌 엔티티에서 사용하기 위한 인증서를 발급합니다.중간 CA 서버 - 중간 또는 발급 CA 서버는 다른 CA 서버가 아닌 엔티티에서 사용하기 위한 인증서를 발급합니다.
- MMC(Microsoft Management Console) - 다양한 스냅인을 로드할 수 있도록 Microsoft Windows에 포함된 응용 프로그램입니다.스냅인을 사용하여 서버 관리를 위한 사용자 지정 콘솔을 만들 수 있습니다.Windows에는 다양한 스냅인이 포함되어 있습니다.인증서, 장치 관리자, 디스크 관리, 이벤트 뷰어 및 서비스 등의 간단한 예가 있습니다.
- NLB(Network Load Balancer) - 여러 물리적 리소스를 일반 물리적 이름으로 최종 사용자에게 표시하는 장치 또는 응용 프로그램입니다.NLB는 웹 응용 프로그램 및 서비스와 매우 공통적입니다.NLB는 여러 가지 방법으로 구현할 수 있습니다.ECE와 함께 사용할 경우 쿠키 삽입 또는

동일한 방법을 사용하여 사용자 세션이 동일한 물리적 백 엔드 웹 서버로 돌아갈 수 있도록 NLB를 구성해야 합니다.이를 쿠키 삽입이 있는 스티키 세션이라고 합니다.스티커 세션은 모든 상호 작용에 대해 사용자의 세션을 동일한 물리적 백엔드 서버로 반환하는 로드 밸런서의 기능을 의미합니다. SSL(Secure Sockets Layer) Passthrough - SSL 패스스루는 최종 사용자 디바이스와 사용자의 세션이 할당된 물리적 웹 서버 간에 SSL 세션이 존재하는 방법입니다.HTTP 세션이 항상 물리적으로 암호화되므로 SSL 패스스루에서는 쿠키 삽입을 허용하지 않습니다.대부분의 NLB는 세션 설정의 serverhello 및 clientello 부분을 모니터링하고 테이블에 고유한 값을 저장하는 스틱 테이블을 사용하여 SSL 패스스루에서 고정 세션을 지원합니다.이러한 값과 일치하는 다음 요청이 NLB에 표시되면 스틱 테이블을 사용하여 세션을 동일한 백 엔드 서버로 반환할 수 있습니다.SSL 오프로드 - NLB가 SSL 오프로드용으로 구성된 경우 지정된 최종 사용자 세션에 대해 두 개의 SSL 세션 또는 터널이 존재합니다.첫 번째는 웹 사이트의 NLB에 구성된 VIP(가상 IP)와 최종 사용자 장치 사이에 있습니다.두 번째는 NLB의 백 엔드 IP와 사용자 세션이 할당된 물리적 웹 서버 사이에 있습니다.SSL 오프로드는 HTTP 스트림이 완전히 해독되는 동안 NLB에서 추가 HTTP 쿠키를 삽입하고 세션 검사를 수행할 수 있으므로 쿠키 삽입을 지원합니다.SSL 오프로드는 웹 애플리케이션에 SSL이 필요하지 않지만 보안을 위해 수행되는 경우에 자주 사용됩니다.현재 버전의 ECE는 비 SSL 세션에서 애플리케이션에 대한 액세스를 지원하지 않습니다.

전제 조건 단계

두 시스템을 통합하기 전에 완료해야 하는 몇 가지 전제 조건이 있습니다.

- 최소 PCCE 패치 레벨 버전 12.0(1) - ES37버전 12.5(1) - 기본 기능에 대한 현재 최소 버전이 없습니다.
  WXM(Webex Experience Management) Analyzer 기능을 사용하려면 ES7이 필요함
- 최소 ECE 패치 레벨 ECE에서 최신 엔지니어링 특별 광고(ES)를 실행하는 것이 좋습니다.버전 12.0(1) - ES3 + ES3_ET1a버전 12.5(1) - 기본 기능에 대한 현재 최소 버전이 없습니다.
  WXM Analyzer 기능을 사용하려면 ES1 필요
- 구성 항목 ECE_Email, ECE_Chat 및 ECE_Outbound Media Routing Domains(MRD)를 올바른 애플리케이션 인스턴스와 연결하는지 확인합니다.PCCE 2000 에이전트 구축 모델의 경우 애플리케이션 인스턴스는 MultiChannel입니다.PCCE 4000/12000 에이전트 배포 모델의 경우 응용 프로그램 인스턴스는 {site}_{peripheral_set}_{application_instance} 형식입니다.
  사이트 이름이 Main이고 주변 장치가 PS1로 설정되고 애플리케이션 인스턴스가 Multichannel로 설정된 PCCE를 설치한 경우 애플리케이션 인스턴스 이름은 Main_PS1_Multichannel입니다.**참고:**애플리케이션 인스턴스 이름은 대/소문자를 구분합니다.인벤토리에 ECE 웹 서버를 추가할 때 이름을 올바르게 입력해야 합니다.

통합 단계

이 문서의 모든 단계에 대한 세부 정보는 모두 ECE와 PCCE에 대한 설명서에서 다루어지지만 목록에 표시되지 않으며 모두 동일한 문서에 포함되어 있지 않습니다.자세한 내용은 이 문서의 끝에 포함된 링크를 참조하십시오.

1단계. SSL 인증서 구성

ECE 웹 서버에서 사용할 인증서를 생성해야 합니다.자체 서명 인증서를 사용할 수 있지만 CA 서명 인증서를 사용하는 것이 더 쉬운 경우가 많습니다.자체 서명 인증서는 CA 서명 인증서보다 안전하

지 않으며, 인증서를 처음 생성하는 단계는 더 적지만, 인증서를 교체해야 하는 경우 모든 PCCE 관리 데이터 서버의 Java 키 저장소에 새 인증서를 업로드해야 합니다.CA 서명 인증서를 사용하는 경우 루트 및 중간 인증서가 있는 경우에만 키 저장소에 업로드해야 합니다.

구축에 여러 웹 서버가 있는 경우 이 지침을 검토해야 합니다.네트워크 부하 분산 장치를 구성하는 데 필요한 특정 단계는 이 문서의 범위를 벗어납니다.필요한 경우 로드 밸런서 공급업체에 문의하십시오.

필수 사항은 아니지만 로드 밸런서는 구현을 크게 간소화합니다.

각 웹 서버에서 ECE 애플리케이션에 액세스하려면 사용된 로드 밸런서 방법에 관계없이 SSL을 사용해야 합니다.

로드 밸런서는 SSL 통과 또는 SSL 오프로드로 구성할 수 있습니다.

SSL 패스스루를 선택한 경우 다음을 수행해야 합니다.한 서버에서 모든 인증서 작업을 수행해야 합니다.

인증서가 올바르게 구성되면 인증서를 내보내고 개인 키가 PFX(개인 정보 교환) 파일에 포함되어 있는지 확인해야 합니다

배포의 다른 모든 웹 서버에 PFX 파일을 복사한 다음 IIS로 인증서를 가져와야 합니다.

SSL 오프로드를 선택한 경우 각 웹 서버가 자체 개별 SSL 인증서로 구성될 수 있습니다.

> **참고:**웹 서버가 여러 개인 경우 웹 서버에서 SSL 패스스루를 선택하거나 모든 서버에서 공통 인증서를 사용하려는 경우 1단계를 수행할 웹 서버 하나를 선택한 다음 인증서를 다른 모든 웹 서버로 가져와야 합니다.
> SSL 오프로드를 선택하는 경우 모든 웹 서버에서 이 단계를 수행해야 합니다.또한 로드 밸런서에서 사용할 인증서를 생성해야 합니다.

1.1단계. 인증서 생성

이미 인증서를 생성했거나 취득한 경우 이 섹션을 건너뛸 수 있습니다. 그렇지 않은 경우 두 옵션 중 하나를 선택합니다.

옵션 1. 자체 서명 인증서 사용

1. IIS 관리로 이동합니다.
2. 왼쪽의 연결 트리에서 서버 이름을 선택합니다.
3. 가운데 창에서 Server Certificates를 찾아 두 번 클릭하여 엽니다.
4. 오른쪽 **Actions(작업) 창에서 Create Self-Signed Certificate...**를 선택합니다.
5. Create **Self-Signed Certificate(자체 서명 인증서 생성**) 창에서 Specify a friendly name for the certificate(**인증서의 식별 이름 지정)**에서 이름**을** 선택하고 **입력합니다.**상자.이 이름은 다음 주요 단계의 선택 프로세스에 인증서가 표시되는 방법입니다.이 이름은 인증서의 일반 이름과 일치할 필요가 없으며 인증서가 최종 사용자에게 표시되는 방식에는 영향을 주지 않습니다.
6. Select a certificate store for the **new certificate**(**새 인증서**에 **대한 인증서 저장소 선택)에서**

Personal(개인)이 선택되었는지 확인합니다.드롭다운 상자
7. 확인을 선택하여 인증서를 생성합니다.
8. 다음 주요 단계인 **웹 사이트에 인증서 바인딩으로 진행합니다**.

옵션 2. CA 서명 인증서 사용

CA 서명 인증서는 CSR(Certificate Signing Request)을 생성해야 합니다. CSR은 CA로 전송된 텍스트 파일로, CA에 서명된 인증서와 함께 필수 CA 인증서가 반환되고 CSR이 이행됩니다.IIS 관리 또는 MMC(Microsoft Management Console)를 통해 이 작업을 수행하도록 선택할 수 있습니다. IIS 관리 방법은 특별한 지식이 없어도 훨씬 쉽게 사용할 수 있지만 인증서의 Subject 특성에 포함된 필드만 구성하고 비트 길이를 변경할 수 있습니다.MMC는 추가 단계를 수행해야 하며 유효한 CSR에 필요한 모든 필드에 대해 철저히 알고 있어야 합니다.인증서 만들기 및 관리에 대해 보통 수준 이상의 경험을 가진 경우에만 MMC를 사용하는 것이 좋습니다.구축에서 둘 이상의 정규화된 이름으로 ECE에 액세스해야 하거나 제목과 비트 길이를 제외한 인증서의 일부를 변경해야 하는 경우 MMC 방법을 사용해야 합니다.

1. IIS 관리를 통해 다음 단계를 사용하여 IIS 관리자를 통해 CSR(Certificate Signing Request)을 생성합니다.IIS 관리로 이동합니다.왼쪽의 연결 트리에서 서버 이름을 선택합니다.가운데 창에서 Server Certificates를 찾아 두 번 클릭하여 엽니다.오른쪽 **Actions(작업**) 창에서 Create Certificate Request(인증서 요청 생성)..를 선택합니다.인증서 **요청** 마법사가 나타납니다.Distinguished **Name Properties** 페이지에서 시스템의 양식에 값을 입력합니다.모든 필드를 입력해야 합니다.계속하려면 **다음**을 선택합니다.암호화 **서비스 제공자 속성** 페이지에서 암호화 **서비스 제공자**에 대한 기본 선택 사항**을 유지합니다**.**비트 길이**를 **변경합니다.**최소 **2048**로 **드롭다운합니다**.계속하려면 **다음**을 선택합니다.File **Name** 페이지에서 CSR 파일을 저장할 위치를 선택합니다.CA에 파일을 제공합니다.서명된 인증서를 받으면 웹 서버에 복사하고 다음 단계로 진행합니다.IIS 관리자의 동일한 위치에서 [작업] 창에서 **인증서 요청**을 **완료합니다**.마법사가 나타납니다.Specify **Certificate Authority Response** 페이지에서 CA에서 제공한 인증서를 선택합니다.**이름** 상자에 이름을 지정합니다.이 이름은 다음 주요 단계의 선택 프로세스에 인증서가 표시되는 방법입니다.**새 인증서**에 **대한 인증서 저장소 선택:**드롭다운이 **개인**으로 **설정됩니다**.OK(**확인**)를 선택하여 인증서 업로드를 완료합니다.다음 주요 단계인 **웹 사이트에 인증서 바인딩으로 진행합니다**.
2. MMC(Microsoft Management Console)를 통해 다음 단계를 사용하여 MMC를 통해 CSR을 생성합니다.이 방법을 사용하면 CSR의 모든 측면을 사용자 정의할 수 있습니다.시작 단추를 마우스 오른쪽 단추로 누르고 실행을 선택합니다.실행 상자에 mmc를 입력하고 **확인**을 선택합니다.인증서 스냅인을 MMC 창에 추가합니다. **파일**, 스냅인 **추가/제거...를 선택합니다.**..스냅인 **추가 또는 제거** 상자가 나타납니다.왼쪽의 목록에서 **Certificates**를 **찾아 Add >**를 **선택합니다**.인증서 스냅인 상자가 나타납니다.**컴퓨터 계정** 옵션을 선택한 다음 **>을** 선택합니다.로컬 **컴퓨터**가 **다음**과 **같은지 확인합니다.(이 콘솔이 있는 컴퓨터)**가 **컴퓨터 선택** 페이지에서 선택된 다음 **마침**을 선택합니다.**확인**을 선택하여 스냅인 **추가 또는 제거** 상자**를** 닫습니다.CSR 생성 왼쪽 창에서 **Certificates (Local Computer)(인증서(로컬 컴퓨터))**를 **Personal(개인)**을 확장하고 **Certificates(인증서**) 폴더를 선택합니다.**인증서** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **All Tasks(모든 작업) > Advanced Operations(고급 작업) >**로 이동한 다음 **Create Custom Request...를 선택합니다.**.Certificate **Enrollment** 마법사가 나타납니다.소개 화면에서 Next를 선택합니다.Select **Certificate Enrollment Policy**(인증서 등록 정책 선택) 페이지에서 Custom Request(사용자 지정 요청) 아래에 나열된 **Proceed without enrollment policy(등록 정책** 없이 진행)를 선택한 다음 **Next(다음)를** 선택합니다.Custom **request**(사용자 지정 **요청**) 페이지에서 **Template(템플릿** 없음) **CNG 키가** 선택되어 있는지, **Request** 형식이 CA에 적합한지 확인합니다.**PKCS #10**은 Microsoft CA에서 작동합니다.다음 페이지를 진행하려면 다음을 선택합니다.Certificate **Information** 페이지에서 **Details** 단어 옆에 있는 드롭다운을 선택하고 **Properties** 버

튼을 선택합니다.Certificate **Properties** 폼이 나타납니다.**인증서 속성** 양식에 대한 모든 옵션을 제공하는 것은 이 문서의 범위를 벗어납니다.자세한 내용은 Microsoft 설명서를 참조하십시오.여기 이 양식에 대한 몇 가지 참고 사항과 팁이 있습니다. **제목 이름**에 필요한 모든 값을 입력했는지 **확인합니다.제목**의 섹션:탭**일반 이름**에 대해 제공된 값이 **대체 이름**에 제공되는지 **확인합니다.**섹션**유형**을 설정합니다.**DNS**에 URL을 **값**에 **입력합니다.**상자를 선택한 다음 **Add >** 버튼**을** 선택합니다.여러 URL을 사용하여 ECE에 액세스하려면 이 필드에 각 대체 이름을 입력하고 각각 **Add >**를 선택합니다.**개인 키** 탭의 **키 크기**를 1024보다 큰 값으로 설정해야 합니다.HA 설치에서 자주 수행하는 것처럼 여러 웹 서버에서 사용할 인증서를 내보내려는 경우 **개인 키 내보내기 가능**을 선택해야 합니다.이렇게 하지 않으면 나중에 인증서를 내보낼 수 없습니다.입력한 값과 선택한 값이 검증되지 않습니다.모든 필수 정보를 제공해야 합니다. 그렇지 않으면 CA가 CSR을 완료할 수 없습니다.모든 항목을 선택했으면 **확인**을 선택하여 마법사로 돌아갑니다.다음 페이지를 진행하려면 다음을 선택합니다.**오프라인 요청**을 **저장할 위치**페이지에서 액세스할 수 있는 위치에서 파일 이름을 선택합니다.대부분의 CA에서 **Base 64**를 형식으로 선택해야 합니다.CA에 파일을 제공합니다.사용자가 서명하고 인증서를 반환하면 인증서를 웹 서버에 복사하고 마지막 단계를 진행합니다.MMC용 인증서 관리 스냅인에서 **인증서(로컬 컴퓨터) > 개인**으로 이동하여 **인증서**를 마우스 오른쪽 단추로 클릭한 다음 **모든 작업 > 가져오기...를 선택합니다.**.Certificate **Import Wizard가** 나타납니다.소개 화면에서 다음을 선택합니다.가져올 **파일** 화면에서 CA에서 서명한 인증서를 선택한 다음 **다음**을 선택합니다.**다음 저장소**에 **모든 인증서 저장을** 선택해야 합니다.**인증서 저장소**에서 **개인**이 선택되었는지 확인합니다.상자를 선택한 다음 **다음을** 선택합니다.최종 화면을 검토한 다음 **Finish**(**마침**)를 선택하여 가져오기를 완료합니다.이제 MMC 콘솔을 닫을 수 있습니다.콘솔 설정을 저장하라는 메시지가 표시되면 **아니오**를 선택할 수 있습니다. 인증서 가져오기에는 영향을 주지 않습니다.다음 주요 단계인 **웹 사이트에 인증서 바인딩으로 진행합니다**.

1.2단계. 웹 사이트에 인증서 바인딩

주의: Edit Site Binding(사이트 바인딩 편집) 상자에서 호스트 이름 필드가 비어 있고 Require Server Name Indication(서버 이름 표시 필요) 옵션이 선택되어 있지 않은지 확인해야 합니다.이 중 하나가 구성된 경우 ECE와의 통신을 시도할 때 SPOG가 실패합니다.

1. 이전에 IIS(인터넷 정보 서비스) 관리자를 열지 않은 경우 엽니다.
2. 왼쪽 **Connections** 창에서 **Sites**로 이동하고 **Default Web Site**를 **선택합니다**. 기본 웹 사이트 이외의 사이트 이름을 사용하도록 선택한 경우 올바른 사이트 이름을 선택해야 합니다.
3. 오른쪽 **Actions** 창에서 Bindings**..**를 선택합니다.사이트 **바인딩** 상자가 나타납니다. **Type**, https 및 **Port**, **443**의 행이 없으면 다음을 완료합니다.그렇지 않으면 다음 주요 단계로 진행합니다. Add**...** 버튼을 선택하면 **Add Site Binding** 상자가 나타납니다.유형에서 https를 **선택합니다.**드롭다운.**IP 주소**가 다음**과 같은지 확인합니다.**드롭다운에는 All Unassigned(**모든 미할당**) 및 Port(포트)가 **표시됩니다.**필드는 **443입니다**.**호스트 이름**을 그대로 두어야 합니다.**필드가 비어 있고 **Require Server Name Indication** 옵션**이 선택되지** 않았습니다.**SSL 인증서**에서드롭다운에서 이전에 생성한 인증서 이름에 해당하는 인증서 이름을 선택합니다. 어떤 인증서를 선택해야 할지 확실하지 않은 경우 **선택...** 버튼을 사용하여 서버에 있는 인증서를 보고 검색합니다.보기 **...** 버튼을 사용하여 선택한 인증서를 보고 세부사항이 올바른지 확인합니다.확인**을** 선택하여 선택 사항을 저장합니다.Type(유형) 열**에 https**를 표시하는 행을 선택한 다음 Edit(편집)... 버튼**을** 선택합니다.사이트 **바인딩 편집** 상자가 나타납니다. **IP 주소**가 다음**과 같은지 확인합니다.**드롭다운에는 All Unassigned(**모든 미할당**) 및 Port(포트)가 **표시됩니다.**필드는 **443입니다**.**호스트 이름**이 다음**과 같은지 확인합니다.**필드가 비어 있고 **서버 이름 표시 필요** 옵션이 선택되지 않았습니다.**SSL 인증서**에서드롭다운에서 이전에 생성한 인증서 이름에 해당하는

인증서 이름을 선택합니다. 어떤 인증서를 선택해야 할지 확실하지 않은 경우 **선택...** 버튼을 사용하여 서버에 있는 인증서를 보고 검색합니다.보기 **...** 버튼을 사용하여 선택한 인증서를 보고 세부사항이 올바른지 확인합니다.확인**을** 선택하여 선택 사항을 저장합니다.IIS 관리자로 돌아가려면 닫기를 선택합니다.

4. 이제 IIS 관리자를 닫을 수 있습니다.

2단계. 파티션 관리자 SSO 구성

파티션 관리자 SSO 컨피그레이션을 사용하면 ECE는 SPOG에서 ECE 가젯을 여는 모든 관리자에 대해 파티션 레벨 사용자 계정을 자동으로 생성할 수 있습니다.

참고:에이전트 또는 수퍼바이저 SSO를 활성화하지 않으려는 경우에도 파티션 관리자 SSO를 구성해야 합니다.

2.1단계. AD(Active Directory) 인증서를 가져오고 키 저장소를 만듭니다.

이 단계는 Microsoft에서 발표한 최신 보안 변경 사항을 해결하기 위해 필요합니다.

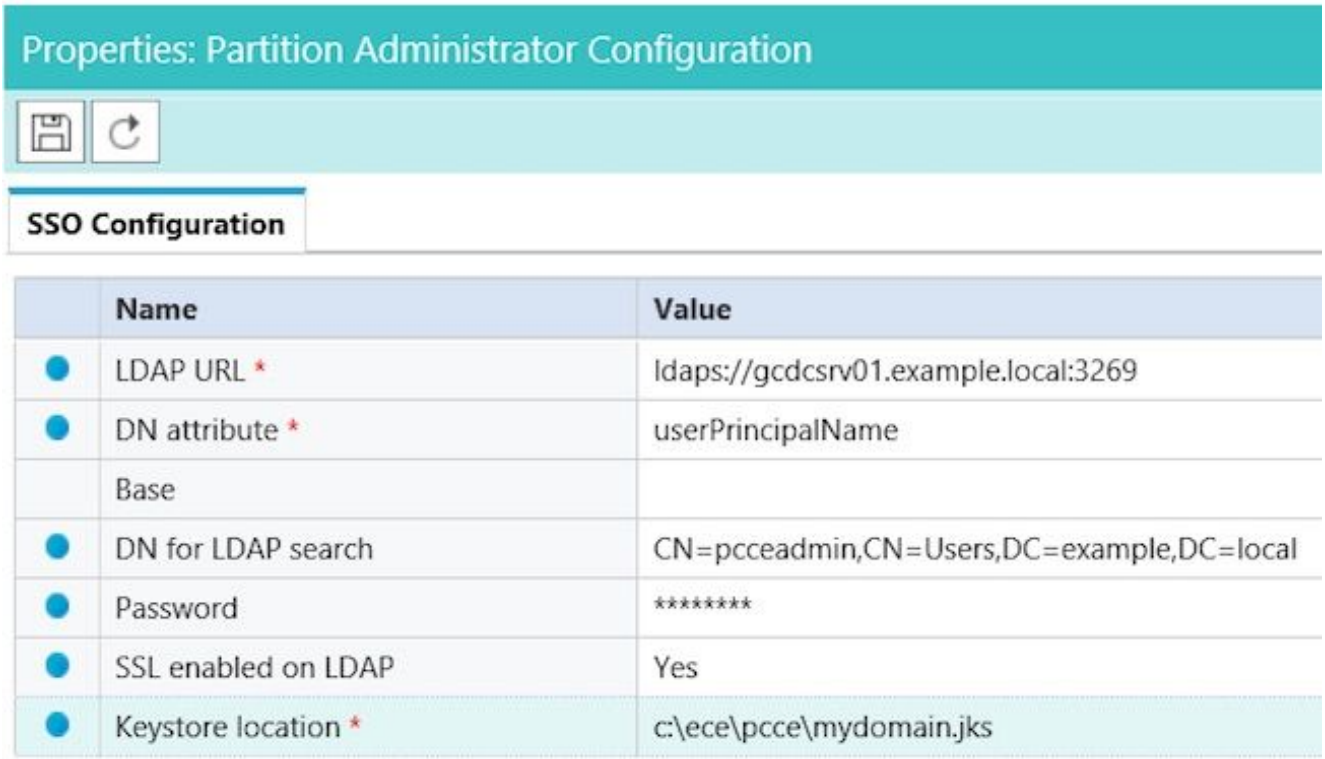
자세한 내용은 https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows을 참조하십시오.

1. Partition Administrator Configuration(파티션 관리자 컨피그레이션) 양식에 제공하는 AD 서버에서 Base 64 형식의 SSL 인증서를 가져옵니다.
2. 인증서 파일을 애플리케이션 서버 중 하나에 복사합니다.
3. 인증서를 복사한 응용 프로그램 서버에 대한 RDP 세션을 엽니다.
4. 다음과 같이 새 Java 키 저장소를 생성합니다. 응용 프로그램 서버에서 명령 프롬프트를 엽니다.ECE JDK(Java Development Kit) bin 디렉토리로 변경합니다.이 명령을 실행합니다.값을 적절하게 바꿉니다.
   keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. 사용자 환경의 다른 모든 Application Server에 있는 동일한 경로에 키 저장소를 복사합니다.

2.2단계. AD LDAP(Lightweight Directory Access Protocol) 액세스 정보로 ECE를 구성합니다.

1. **Internet Explorer 11**이 있는 워크스테이션 또는 컴퓨터에서 Business 파티션 URL로 이동합니다. **팁**:비즈니스 파티션은 파티션 1이라고도 합니다. 대부분의 설치에서 비즈니스 파티션은 https://ece.example.com/default과 유사한 URL을 통해 액세스할 수 있습니다.
2. pa로 로그인하여 시스템의 비밀번호를 입력합니다.
3. 성공적으로 로그인했으면 초기 콘솔에서 **Administration**(관리) 링크를 선택합니다.
4. 다음과 같이 **SSO Configuration** 폴더, Administration(관리) **> Partition(파티션)으로 이동합니다.default(기본값) > Security(보안) > SSO and Provisioning(SSO 및 프로비저닝)**.
5. 오른쪽 상단 창에서 파티션 관리 구성 **항목을** 선택합니다.
6. 오른쪽 하단 창에 LDAP(Lightweight Directory Access Protocol) 및 AD의 값을 입력합니다.
   LDAP URL - 모범 사례로서 GC(Global Catalog) 도메인 컨트롤러의 이름을 사용합니다.
   GC를 사용하지 않으면 ApplicationServer 로그에 다음과 같은 오류가 표시될 수 있습니다.
   LDAP 인증의 예외 <@>
   javax.naming.PartialResultException:처리되지 않은 연속 참조;나머지 이름

'DC=example,DC=com' 비보안 글로벌 카탈로그 포트는 3268입니다.보안 글로벌 카탈로그 포트는 3269입니다.**DN 특성** - userPrincipalName이어야 합니다.**Base** - GC를 사용하는 경우에는 필요하지 않습니다. 그렇지 않으면 기본 적절한 LDAP 형식을 제공해야 합니다.**LDAP 검색을 위한 DN** - 도메인이 익명 바인딩을 허용하지 않는 한 LDAP에 바인딩하고 디렉토리 트리를 검색할 수 있는 기능을 가진 사용자의 고유 이름을 제공해야 합니다.
팁 - 사용자의 올바른 값을 찾는 가장 쉬운 방법은 Active Directory 사용자 및 컴퓨터 도구를 사용하는 것입니다. 보기 메뉴에서 **고급 기능을** 활성화합니다.사용자 객체로 이동한 다음 마우스 오른쪽 단추를 누르고 등록 정보를 **선택합니다**.속성 탭을 **선택합니다**.필터 버튼을 선택한 다음 **값이 있는 속성만 표시를 선택합니다**.목록에서 distinguishedName을 찾은 다음 두 번 클릭하여 값을 봅니다.표시된 값을 강조 표시한 다음 복사하여 텍스트 편집기에 붙여넣습니다.텍스트 파일의 값을 복사하여 **DN for LDAP search** 필드에 붙여넣습니다.
값은 CN=pcceadmin, CN=Users, DC=example, DC=local과 유사해야 합니다.**비밀번호** - 도메인이 익명 바인딩을 허용하지 않는 한 사용자가 지정한 비밀번호를 제공해야 합니다.**LDAP에서 SSL 사용** - 이 필드는 대부분의 고객에게 필수 항목으로 간주해야 합니다.**키 저장소 위치** - AD에서 SSL 인증서를 가져온 키 저장소의 위치여야 합니다.이 예에서는 c:\ece\pcce\mydomain.jks이며, 이미지에 나와 있습니다.



7. 플로피 디스크의 아이콘을 선택하여 변경 사항을 저장합니다.

3단계. 구성 파일 검증

모든 12.0 설치에는 이 섹션을 반드시 완료해야 합니다.12.0이 아닌 모든 버전의 경우 이 섹션을 건너뛸 수 있습니다.
이 단계가 필요할 수 있는 두 가지 추가 시나리오가 있습니다.첫 번째는 ECE를 고가용성 설정에 설치한 경우입니다.두 번째이자 더 일반적인 것은 웹 서버의 호스트 이름이 ECE에 액세스하는 데 사용하는 이름과 일치하지 않을 때 발생합니다.예를 들어, 호스트 이름 UCSVREWEB.example.com으로 서버에 ECE 웹 서버를 설치하지만 사용자가 URL chat.example.com으로 ECE 웹 페이지에 액세스하는 경우 이 섹션을 완료해야 합니다.서버의 호스트 이름과 ECE에 액세스하는 URL이 동일하고 버전 12.5 이상을 설치한 경우 이 단계를 건너뛰고 섹션을 완료할 수 있습니다.

{ECE_HOME}을(를) ECE를 설치한 물리적 위치로 바꿉니다.예를 들어 ECE를 C:\Cisco에 설치한 경우 각 위치에서 {ECE_HOME}을 **C:\Cisco**로 바꿉니다.

> **팁**:메모장이나 워드패드 대신 Notepad++와 같은 텍스트 편집기를 사용하면 줄 끝을 제대로 해석하지 않습니다.

1. 구축의 모든 ECE 웹 서버에 대한 원격 데스크톱 세션을 엽니다.
2. 이 경로, **{ECE_HOME}\eService\templates\finesse\gadget\spog으로 이동합니다**.
3. spog_**config.**jsfile을 찾아 안전한 위치에 백업 복사본을 만듭니다.
4. 현재 spog_**config.**jsfile을 텍스트 편집기에서 엽니다.
5. 이 두 행을 찾아 구축에 맞게 업데이트합니다.
   web_server_protocol은 https여야 하며 필요한 경우 업데이트합니다.
   ECE에 액세스하는 데 사용하도록 할당한 정규화된 이름과 일치하도록 web_server_name을 업데이트합니다.예:**ece.example.com** var web_server_protocol = "https";var web_server_name = "ece.example.com";
6. 변경 사항을 저장합니다.
7. 구축의 다른 모든 웹 서버에서 반복합니다.

4단계. PCCE 인벤토리에 ECE 추가

12.0부터 PCCE에는 3가지 배포 옵션, 2000개의 에이전트(2K 에이전트), 4000개의 에이전트(4K 에이전트) 및 12000개의 에이전트(12K 에이전트)가 있습니다. 이러한 3가지 구축 옵션은 2K Agent와 4K/12K Agent의 두 그룹으로 구분할 수 있습니다.SPOG의 모양에 몇 가지 근본적인 차이가 있기 때문에 이러한 방식으로 구분됩니다.이 단락을 따라 두 방법을 매우 개괄적으로 비교합니다.이 문서에서는 인벤토리에 구성 요소를 추가하는 특정 단계를 제공하지 않습니다.이 프로세스에 대한 자세한 내용은 이 문서의 끝에 있는 링크를 참조하십시오.이 섹션에서는 PCCE에 ECE를 추가할 때 검증해야 하는 특정 세부 정보에 대해 설명합니다. 또한 PCCE 설치가 완료되었으며 솔루션의 다른 측면에 액세스하고 구성할 수 있다고 가정합니다.

- 2K 에이전트 구축 PCCE 구성 요소의 초기 컨피그레이션은 전적으로 CCE 관리를 통해 이루어지며 자동화됨IP 또는 호스트 이름 및 필요한 자격 증명 또는 구성 요소별 컨피그레이션과 같은 세부사항을 입력하는 팝업 상자를 통해 Inventory(인벤토리) 페이지에 새 구성 요소가 추가됩니다.
- 4K 및 12K 에이전트 구축 초기 컨피그레이션의 상당 부분이 UCCE에 사용되는 단계를 미러링합니다.CCE 관리에서 다운로드한 CSV(Comma-Separated Values) 파일을 통해 구성 요소가 추가되고, 특정 설치에 따라 입력한 다음 업로드합니다.초기 구축에서는 첫 번째 CSV 파일에 일부 특정 구성 요소를 포함해야 합니다.시스템이 처음 설정되었을 때 추가되지 않은 구성 요소는 필요한 정보가 포함된 CSV 파일을 통해 추가됩니다

4.1단계. Java Keystore에 ECE 웹 서버 인증서 업로드

1. 자체 서명 인증서를 사용하는 경우 기본 ADS(Side-A Administration Data Server)에 대한 원격 데스크톱 연결을 엽니다.Internet Explorer 11을 관리자로 열고 ECE 비즈니스 파티션으로 이동합니다.URL 표시줄 오른쪽에 있는 자물쇠 아이콘을 선택한 다음 **View Certificates**(인증서 보기)를 선택합니다.Certificate(**인증서**) 상자에서 Details(**세부사항**) 탭을 선택합니다.탭 하단**에서 파일에 복사...**를 선택합니다.Certificate **Export Wizard(인증서 내보내기 마법사**)에서 Export File Format(**파일 내보내기 형식**) 페이지에 도달할 때까지 Next(다음)를 선택합니다.**Base-64 인코딩 X.509(.CER)** 형식**을** 선택해야 합니다.인증서를 ADS 서버의

c:\Temp\certificates과 같은 위치에 저장하여 내보내기를 완료합니다.다른 모든 ADS 서버에 인증서를 복사합니다.관리 명령 프롬프트를 엽니다.Java 홈 디렉토리로 변경한 다음 bin 디렉토리로 변경합니다.Java 홈 디렉토리는 다음과 같이 액세스할 수 있습니다.**cd %JAVA_HOME%\bin**현재 캐시 파일**을** 백업합니다.**%JAVA_HOME%\lib\security**에서 다른 위치**로** 캐시 파일을 복사합니다.이전에 저장한 인증서를 가져오려면 이 명령을 실행합니다.키 저장소 암호가 'changeit'가 아닌 경우 명령을 업데이트하여 설치를 확인합니다.
keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <ECE 서버의 FQDN> -file <인증서를 저장한 위치>ADS 서버를 다시 시작합니다.다른 ADS 서버에서 8-12단계를 반복합니다.

2. CA 서명 인증서를 사용하는 경우 루트 및 중간 인증서를 DER/PEM 형식으로 가져와 모든 ADS 서버의 C:\Temp\certificates과 같은 위치에 복사합니다. **참고:**이러한 인증서를 얻으려면 CA 관리자에게 문의하십시오. 기본 A측 ADS에 대한 원격 데스크톱 연결을 엽니다.관리 명령 프롬프트를 엽니다.Java 홈 디렉토리로 변경한 다음 bin 디렉토리로 변경합니다.Java 홈 디렉토리는 다음과 같이 액세스할 수 있습니다.**cd %JAVA_HOME%\bin**현재 캐시 파일**을** 백업합니다.**%JAVA_HOME%\lib\security**에서 다른 위치**로** 캐시 파일을 복사합니다.이전에 저장한 인증서를 가져오려면 이 명령을 실행합니다.키 저장소 암호가 'changeit'가 아닌 경우 명령을 업데이트하여 설치를 확인합니다.
keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <CA 루트 이름> -file <루트 인증서를 저장한 위치>6단계를 반복하고 중간 인증서가 있으면 가져옵니다.ADS 서버를 다시 시작합니다.다른 모든 ADS 서버에서 2-12단계를 반복합니다.

4.2단계. 인벤토리에 ECE 데이터 서버 추가

- 데이터 서버가 시스템 인벤토리에 있어야 하지만 PCCE ADS와 데이터 서버 간에 직접적인 통신이 이루어지지 않습니다
- ECE가 1500 에이전트 구축에 구축되면 데이터 서버는 서비스 서버입니다.
- ECE가 HA 컨피그레이션에 설치된 경우 두 서비스 서버를 모두 추가해야 합니다.

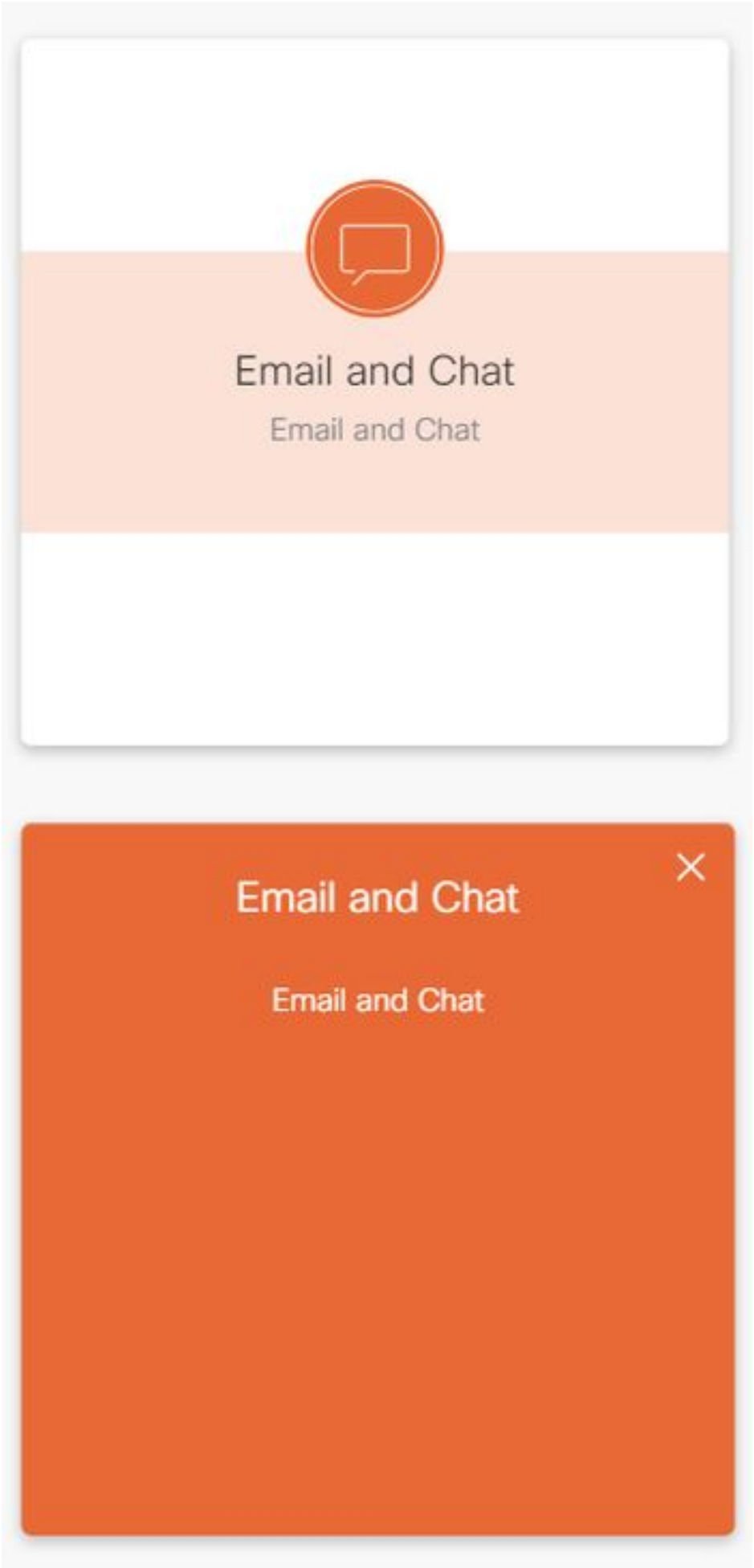
4.3단계. 인벤토리에 ECE 웹 서버 추가

- 정규화된 이름으로 웹 서버를 추가했는지 확인합니다. 이 이름은 ECE 인증서의 일반 이름과 일치하거나 SAN(Subject Alternative Name) 중 하나로 나열되어야 합니다.호스트 이름 또는 IP 주소만 사용하면 안 됩니다.
- ECE의 사용자 이름과 비밀번호는 pa 로그인 자격 증명이어야 합니다.
- 애플리케이션 인스턴스가 올바른지 확인합니다. 애플리케이션 인스턴스 이름은 대/소문자를 구분합니다.2000 Agent PCCE 구축의 경우 애플리케이션 인스턴스는 MultiChannel입니다.4000/12000 에이전트 PCCE 구축의 경우 애플리케이션 인스턴스에는 이름의 일부로 설정된 사이트 및 주변 장치가 포함됩니다
- ECE가 둘 이상의 웹 서버와 함께 설치된 경우(예: 1500 Agent 구축 또는 400 Agent HA 구축) 로드 밸런서를 가리키는 URL 또는 각 개별 웹 서버를 웹 서버의 정규화된 이름으로 가리키는 URL을 사용할 수 있습니다.
- 둘 이상의 ECE 구축이 있거나 둘 이상의 구축에서 각 개별 웹 서버를 추가하도록 선택한 경우 SPOG에서 ECE 가젯을 열 때 올바른 웹 서버를 많이 선택합니다.

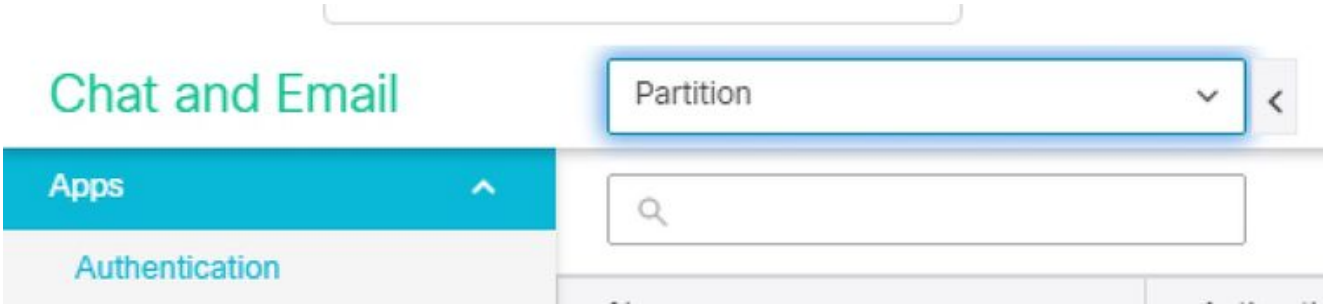
5단계. ECE를 PCCE와 통합

1. CCE Administration에 관리자로 로그인합니다.

2. 이미지에 표시된 대로 **이메일 및 채팅** 카드를 선택한 다음 **이메일 및 채팅** 링크를 선택합니다.



3. Device Name(디바이스 이름) 드롭다운에서 현재 선택한 서버를 검토합니다.HA 설치에서 두 웹 서버를 모두 추가한 경우 웹 서버 중 하나를 선택할 수 있습니다.나중에 시스템에 두 번째 ECE 구축을 추가하는 경우 계속하기 전에 적절한 서버를 선택해야 합니다.
4. Chat **and Email**(채팅 **및 이메일**) 옆의 드롭다운에서 이미지에 표시된 대로 **Partition** 또는 **Global(전역)**을 선택합니다.



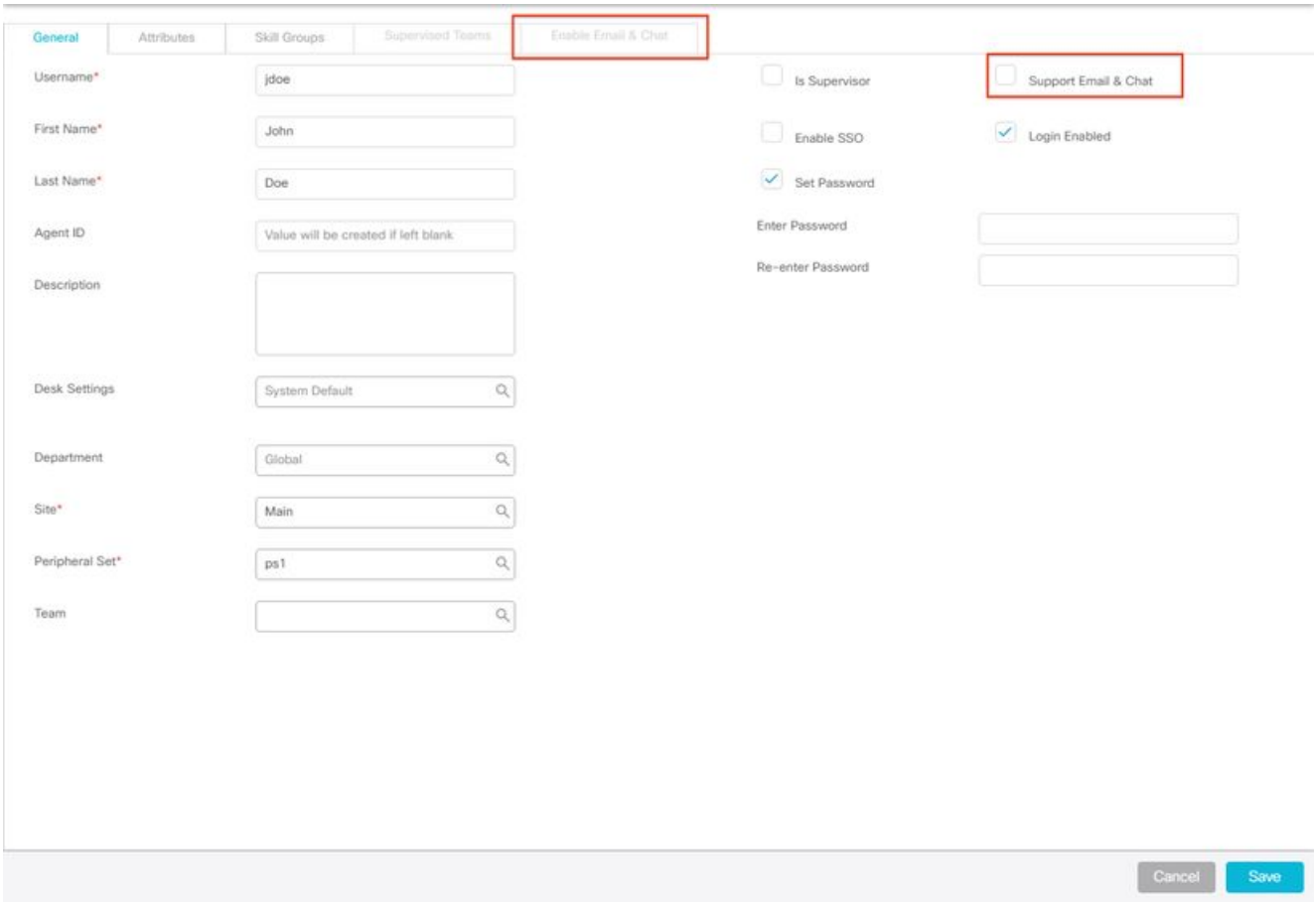
5. 상단 메뉴에서 **통합**을 선택한 다음 **Unified CCE** 옆의 화살표를 선택하고 이미지에 표시된 대로 두 번째 **Unified CCE**를 선택합니다.

6. 설치에 대한 AWDB **Details** 탭의 값을 입력한 다음 Save(**저장)** 버튼을 선택합니다.
7. Configuration(컨피그레이션**)** 탭을 선택하고 다음과 같이 이 탭을 완료합니다. Application Instance(애플리케이션 인스턴스) 옆의 드롭다운**을** 선택하고 ECE용으로 생성된 애플리케이션 인스턴스를 선택합니다. **참고:**UQ로 시작하는 애플리케이션 인스턴스는 아니어야 합니다

.흰색 더하기 기호 단추가 있는 녹색 원을 선택합니다. 에이전트 PG를 선택합니다. 에이전트 PG(또는 둘 이상의 경우 에이전트 PG)를 선택합니다.모든 에이전트 PG를 추가한 후 Save(저장)를 선택합니다. **경고:저장**을 선택하면 시스템이 PCCE에 영구적으로 연결되고 실행 취소할 수 없습니다.이 섹션에서 오류가 발생한 경우 ECE를 완전히 제거하고 모든 데이터베이스를 삭제한 다음 ECE를 새로 설치한 것처럼 설치해야 합니다.

6단계. ECE 통합 검증

1. CCE Administration(CCE 관리)에서 상위 상태 표시줄에 경고가 표시되지 않는지 확인합니다. 경고가 있는 경우 **Alerts**라는 단어를 선택하고 Inventory 페이지를 검토하여 ECE 서버에 대한 경고가 없는지 확인합니다.
2. 왼쪽 탐색 모음**에서 Users**(사용자)를 선택한 다음 Agents(에이전트)를 선택합니다.
3. 목록에서 에이전트를 선택하고 이를 확인합니다. 이제 **General** 탭에 **Support Email & Chat(이메일 및 채팅 지원)**에 대한 새 확인란이 표시됩니다.이제 이미지에 표시된 대로 **Enable Email & Chat(이메일 및 채팅 활성화)**라는 새 탭이 표시됩니다.



4. ECE용 테스트 에이전트를 활성화합니다. Support Email **& Chat(이메일 및 채팅 지원**) 확인란을 선택하고 **Enable Email & Chat(이메일 및 채팅 사용**) 탭을 선택할 수 있습니다.Enable **Email & Chat(이메일 및 채팅 활성화**) 탭을 선택하고 Screen Name(**화면 이름**) 필드에 값을 입력합니다.저장**을** 선택하여 사용자를 업데이트합니다.성공 메시지를 수신해야 합니다.
5. ECE가 업데이트되었는지 확인합니다. Overview(**개요**) 탐색 버튼을 선택한 다음 **Email and Chat(이메일 및 채팅** 카드) 및 링크를 선택합니다.채팅 **및 이메일** 옆의 드롭다운에서 상담원의 부서에 해당하는 이름을 선택합니다. **참고:**ECE의 서비스 부서는 PCCE의 글로벌 부서에 속하는 모든 객체를 보유하고 있습니다.따라서 부서 이름 서비스는 예약된 값입니다.상단 메뉴에서 **User Management(사용자 관리)를** 선택한 다음 **Chat and Email(채팅 및 이메일)** 아래의 메뉴에서 Users(사용자)를 **선택합니다**.목록에 새 에이전트가 표시되는지 확인합니다.

문제 해결

여러 툴을 다운로드하고 ECE 서버에 유지하는 것이 좋습니다.따라서 시간이 지남에 따라 솔루션 문제를 훨씬 쉽게 해결하고 유지 관리할 수 있습니다.

- Notepad++ 등의 텍스트 편집기
- 7-Zip과 같은 아카이브 툴
- Windows용 많은 테일 프로그램 중 하나
  예를 들면 다음과 같습니다. Baretail -https://www.baremetalsoft.com/baretail/Win32용 테일 - http://tailforwin32.sourceforge.net/

통합 문제를 해결하려면 먼저 일부 주요 로그 파일과 각 파일의 위치를 알아야 합니다.

1. **ECE의 파일 이름 및 위치**

   ECE 시스템에 많은 로그가 있으며, 이러한 로그는 통합 문제를 해결하려고 시도할 때 가장 유

용합니다.

서버 키:C = 배치된 서버A = 애플리케이션 서버S = 서비스 서버M = 메시징 서버또한 대부분의 로그 파일에는 연결된 다른 두 개의 로그가 있습니다
.eg_log_{SERVERNAME}_{PROCESS}.log - 기본 프로세스 로그
eg_log_dal_conpool_{SERVERNAME}_{PROCESS}.log - 연결 풀 사용량
eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - 시간 초과로 인해 쿼리가 실패할 때 업데이트됩니다.

2. ## PCCE의 파일 이름 및 위치

통합 문제에 대한 PCCE 로그는 모두 A측 ADS에 있습니다.통합 문제를 해결할 때 가장 중요한 로그는 다음과 같습니다.각 파일은 C:\icm\tomcat\logs에 **있습니다**.

이러한 로그 중에서 첫 세 개는 가장 자주 요청되고 검토됩니다.추적 수준을 설정하고 필요한 로그를 수집하려면 다음 단계를 사용합니다.

3. **추적 수준 구성**이 섹션은 ECE에만 적용됩니다.PCCE에서 필요한 로그는 Cisco에서 설정한 추적 레벨을 가지며 변경할 수 없습니다. **Internet Explorer 11**이 있는 워크스테이션 또는 컴퓨터에서 시스템 파티션 URL로 이동합니다. **팁**:시스템 파티션은 파티션 0이라고도 합니다. 대부분의 설치에서 시스템 파티션은 https://ece.example.com/system과 유사한 URL을 통해 액세스할 수 있습니다.sa로 **로그인하고** 시스템의 비밀번호를 입력합니다.성공적으로 로그인했으면 초기 콘솔에서 **System** 링크를 선택합니다.System(**시스템**) 페이지에서 **System(시스템) >** Shared Resources(**공유 리소스**) > Logger(**로거**) > Processes(프로세스)를 **확장합니다.**오른쪽 상단의 창에서 추적 레벨을 변경할 프로세스를 찾아 선택합니다.
참고:HA 시스템과 둘 이상의 애플리케이션 서버가 있는 시스템에서 프로세스가 두 번 이상 나열됩니다.데이터를 캡처하려면 프로세스를 포함하는 모든 서버의 추적 수준을 설정합니다.오른쪽 하단의 창에서 **최대 추적 레벨**에 대한 드롭다운을 선택하고 적절한 값을 선택합니다.
ECE에는 8개의 추적 레벨이 정의되어 있습니다.이 목록의 4는 가장 자주 사용되는 것입니다.
2 - 오류 - 프로세스의 기본 추적 수준4 - 정보 - 문제 해결에 일반적으로 사용되는 추적 레벨6 - Dbquery - 설정 초기 또는 복잡한 문제를 진단하는 데 자주 도움이 됩니다.7 - 디버그 - 매우 자세한 출력, 가장 복잡한 문제에만 필요**참고:**프로세스는 6 - Dbquery에서 장기간 보관하면 안 되며, 일반적으로 TAC 안내에 의해서만 유지됩니다.대부분의 프로세스는 추적 레벨 2-Error로 유지되어야 합니다.레벨 7 또는 8을 선택하는 경우 최대 기간도 선택해야 합니다.최대 지속 시간이 충족되면 추적 수준이 마지막 수준 집합으로 돌아갑니다.
시스템을 설정한 후 이 네 프로세스를 추적 레벨 4로 변경합니다.EAAS 프로세스EAMS-프로세스dx 프로세스rx 프로세스저장 아이콘을 선택하여 새 추적 레벨을 설정합니다.

4. ## 로그 파일 수집

필요한 프로세스 로그가 있는 서버에 대한 원격 데스크톱 세션을 엽니다.로그 파일 위치로 이동합니다. ECE 서버 로그는 다음과 같이 기록됩니다.기본적으로 로그는 최대 크기가 5MB인

파일에 기록됩니다하나의 로그 파일이 구성된 최대값에 도달하면 {LOGNAME}.log 형식으로 이름이 바뀝니다.{#}ECE는 이전 49개의 로그 파일과 현재 파일을 유지합니다.현재 로그는 항상 .log로 끝납니다. 그 다음 숫자는 없습니다.로그가 아카이브되거나 압축되지 않음대부분의 로그에는 공통 구조가 있습니다.로그 파일은 <@>를 사용하여 섹션을 구분합니다.로그는 항상 GMT+0000으로 기록됩니다.ECE 로그는 특정 설치에 따라 다른 위치에 있습니다.400개의 에이전트 구축 단면 서버:배치된 서버위치:**{ECE_HOME}\eService_RT\logs**고가용성 서버:두 개의 배치된 서버위치:**{ECE_HOME}\eService\logs**DFS(분산 파일 시스템) 공유에 대해 만든 디렉터리에는 설치 및 업그레이드를 위한 로그만 포함되어 있습니다.분산 시스템 관리자(DSM) 역할을 소유하는 서버만 서비스 역할의 일부인 구성 요소에 대한 로그를 작성합니다.DSM 역할 소유자는 Windows 작업 관리자의 프로세스 탭에서 찾을 수 있습니다.이 서버에는 보조 서버에 없는 10-15개의 Java 프로세스가 있습니다.DSM의 컴포넌트에는 EAAS, EAMS, Retriever, Dispatcher, Workflow 등이 포함됩니다.1500 에이전트 구축 역할을 호스팅하는 서버에 있는 로그위치:**{ECE_HOME}\eService\logs**서비스 서버를 제외하고 모든 서버는 구성 요소와 연결된 모든 프로세스에 대해 로그를 작동 및 씁니다.고가용성 구축에서 서비스 서버는 액티브/스탠바이 컨피그레이션에서 작동합니다.분산 시스템 관리자(DSM) 역할을 소유하는 서버만 로그를 씁니다.DSM 역할 소유자는 Windows 작업 관리자에 표시되는 프로세스 수로 식별할 수 있습니다.10-15개의 Java 프로세스가 기본 서버에서 실행되며 보조 서버에는 4개의 Java 프로세스만 실행됩니다PCCE 서버 PCCE의 필수 로그는 C:\icm\tomcat\logs에 있습니다.Tomcat 로그는 롤오버 또는 아카이빙되지 않음로그는 로컬 서버 시간으로 기록됩니다.문제가 관찰된 후 생성되거나 수정된 모든 로그를 수집합니다.

로그 및 표시되는 문제에 대한 전체 설명은 이 문서의 범위를 벗어납니다.몇 가지 일반적인 문제, 검토해야 할 사항 및 가능한 해결 방법은 다음과 같습니다. 인증서 관련 문제 인증서를 가져오지 않음 동작:SPOG에서 ECE 가젯을 열려고 하면 "페이지를 로드하는 동안 오류가 발생했습니다.관리자에게 문의하십시오."확인:Catalyst는 PCCE에 이러한 오류와 유사한 오류를 로그온합니다.

javax.net.ssl.SSLHandshakeException:sun.security.validator.validator예외:PKIX 경로 작성 실패:sun.security.provider.certpath.SunCertPathBuilder예외:요청된 대상에 대한 유효한 인증 경로를 찾을 수 없습니다.해결 방법:ECE 웹 서버 인증서 또는 적절한 CA 인증서를 ADS의 키 저장소로 가져왔는지 확인합니다.인증서 불일치 동작:SPOG에서 ECE 가젯을 열려고 하면 인증서의 일반 이름 또는 주체 대체 이름이 구성된 이름과 일치하지 않음을 나타내는 오류가 표시됩니다.확인:SSL 인증서 검증해결 방법:Subject(주체)의 Common Name(공통 이름) 필드 또는 Subject Alternate Name(주체 대체 이름)의 DNS 필드 중 하나에 웹 서버 이름으로 SPOG에 입력한 정규화된 이름이 포함되어 있는지 확인합니다.시스템 문제 서비스가 시작되지 않음 동작:SPOG에서 ECE 가젯을 열려고 하면 "https://{url}의 웹 페이지가 일시적으로 다운되었거나 새 주소로 영구적으로 이동되었을 수 있습니다." 오류가 표시됩니다.확인:웹 서버를 제외하고 모든 ECE 서버에서 Windows 서비스 - Cisco 서비스가 시작되었는지 확인합니다.응용 프로그램 서버의 루트 로그에서 오류를 검토합니다.해결 방법:모든 ECE 서비스에서 Cisco 서비스를 시작합니다.구성 문제 LDAP 컨피그레이션 동작:SPOG에서 ECE 가젯을 열려고 하면 "페이지를 로드하는 동안 오류가 발생했습니다.관리자에게 문의하십시오."확인:Application Server의 추적 수준을 레벨 7- 디버그로 올린 다음 로그인을 다시 시도하고 Application Server 로그를 검토합니다.LDAP라는 단어를 검색합니다.해결 방법:파티션 관리자

SSO에 대한 LDAP 컨피그레이션이 올바른지 확인합니다.

관련 정보

ECE 설치 또는 통합을 시작하기 전에 철저하게 검토해야 하는 주요 문서입니다.ECE 문서의 포괄적인 목록은 아닙니다.

> **주의:**대부분의 ECE 문서에는 두 가지 버전이 있습니다.PCCE용 버전을 다운로드하여 사용해야 합니다.문서 제목에는 Packaged **Contact Center Enterprise용** 또는 **(PCCE의 경우)** 또는 **(UCCE 및 PCCE의 경우)** 버전 번호 뒤에가 있습니다.

설치, 업그레이드 또는 통합 전에 Cisco Enterprise Chat 및 Email 설명서의 시작 페이지에서 모든 업데이트를 확인하십시오.

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

- 12.0 Enterprise Chat and Email 설치 및 구성 가이드엔터프라이즈 채팅 및 이메일 업그레이드 가이드엔터프라이즈 채팅 및 이메일 관리자 가이드
- 12.5 Enterprise Chat and Email 설치 및 구성 가이드엔터프라이즈 채팅 및 이메일 업그레이드 가이드엔터프라이즈 채팅 및 이메일 관리자 가이드