その他のセキュリティに関する検討事項

- その他のシスコ コール センター アプリケーション （1 ページ）
- Java のアップグレード （7 ページ）
- Tomcat ユーティリティのアップグレード, on page 7
- Microsoft セキュリティの更新 （8 ページ）
- Microsoft Internet Information Server（IIS） （9 ページ）
- Active Directory の展開 （9 ページ）
- ネットワークアクセス保護 （11 ページ）
- WMI サービスの強化 （11 ページ）
- SNMP の強化 （12 ページ）
- 電話ハッカーの侵入阻止 （13 ページ）
- サポートされているコンテンツ セキュリティ ポリシー ディレクティブ （14 ページ）
- サードパーティのセキュリティプロバイダー （15 ページ）
- サードパーティ管理エージェント （15 ページ）
- 自己暗号化ドライブ （16 ページ）
- 内部クラウド接続 API エンドポイント （16 ページ）
- 内部 CCE API エンドポイント （18 ページ）

その他のシスコ コール センター アプリケーション

次のセクションでは、他のシスコ コール センター アプリケーションのセキュリティに関する検討事項について説明します。

Cisco Unified ICM ルータ

dbagent.acl ファイルは、内部のバックグラウンドファイルです。このファイルを編集しないでください。ただし、このファイルには読み取りアクセス許可が設定されている必要があります。このファイルを使用すると、ユーザがルータのリアルタイムフィードに接続できます。

周辺機器ゲートウェイ（PG）とエージェントログイン

誤ったパスワードを使用した Unified CCE エージェントログイン試行にはレート制限があります。デフォルトでは、エージェントアカウントは、15 分間で間違ったパスワード試行が 3 回行われると、15 分間無効になります。

このデフォルトは、レジストリキーを使用して変更できます。このレジストリキーは、次の下にあります。`HKLM\SOFTWARE\Cisco Systems, Inc.\\ICM\<inst>\PG(n)[A/B]\PG\CurrentVersion\PIMS\pim(n)\EAGENTData\Dynamic`

レジストリキーには、次のものが含まれます。

- **AccountLockoutDuration**： デフォルト

  ログイン試行が失敗してアカウントがロックアウトされた場合、この値はアカウントがあと何分間ロックアウトされたままかを表します。

- **AccountLockoutResetCountDuration**： デフォルトは 15 です。AccountLockoutThreshold 回数が 0 に戻るまでの時間（分）。これは、アカウントがロックアウトされずに、AccountLockoutThreshold で説明されている値よりも少ないログイン試行が失敗した場合に適用されます。

- **AccountLockoutThreshold**： デフォルトは 3 です。これは、アカウントがロックアウトされた後のログイン試行が失敗した回数です。

（注） これらの設定は、システム周辺機器ゲートウェイを備える CTI OS など、Cisco Finesse 以外のデスクトップソリューションにのみ適用されます。

エージェントまたはスーパーバイザがパスワードを誤って 5 回連続してデスクトップにログインしようとした場合、Finesse はユーザアカウントへのアクセスをブロックします。ロックアウトの時間は 5 分間です。これらの設定の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html にある『*Cisco Finesse* アドミニストレーション ガイド』を参照してください。

エンドポイントセキュリティ

エージェントのデスクトップ（Agent Desktops）

Cisco Finesse は、管理コンソールおよびエージェントおよびスーパーバイザクライアントで HTTPS（TLS 1.2 のみ）をサポートします。

Unified IP Phone デバイスの認証

Contact Center Enterprise ソリューションを設計する際、Cisco Unified IP Phone 向けにデバイス認証を実装できます。Contact Center Enterprise ソリューションは、以下を保証する Unified Communications Manager の 認証済みデバイスセキュリティモードをサポートしています。

- **デバイス ID** — X.509 証明書を使用した相互認証
- **シグナリングインテグリティ** — HMAC-SHA-1 を使用して認証された SIP メッセージ
- **シグナリングプライバシー** — AES-128-CBC を使用して暗号化された SIP メッセージコンテンツ

メディア暗号化（SRTP）の考慮事項

展開で SRTP を有効にする前に以下を考慮してください。

- エージェントレグで安全なメディアを使用するには、インストール済みの IP 電話が SRTP と互換性があることを確認してください。
- 仮想化音声ブラウザは、VRU レグの SRTP をサポートします。
- IOS VXML ゲートウェイは SRTP をサポートしません。
- モバイルエージェントは SRTP を使用できません。
- Cisco アウトバウンドオプション ダイヤラは SRTP をサポートしません。コールがダイヤラに接続されている間、コールは SRTP を使用できません。ただし、コールがダイヤラに接続されなくなると SRTP とネゴシエートできます。

IP Phone の強化

Unified CM の IP Phone デバイス構成では、特定の電話機の機能を無効にすることで電話機を強化できます。たとえば、電話機の PC ポートを無効にしたり、PC による音声 VLAN へのアクセスを制限できます。これら設定の一部を変更すると、Contact Center Enterprise ソリューションの監視機能や録音機能が無効になります。設定は次のように定義されています。

- **PC 音声 VLAN アクセス** — PC ポートに接続されているデバイスを音声 VLAN にアクセスさせるかどうかを電話機が許可しているかを示します。ボイス VLAN アクセスを無効にすると、接続されている PC でボイス VLAN 上のデータを送受信できなくなります。また、電話によって送受信されたデータを PC で受信することもできなくなります。この機能を無効にすると、デスクトップベースの監視と録音が無効されます。

  この設定は有効（デフォルト）です。

- **PC ポートへのスパン** — 電話機が電話機ポートから PC ポートへ送受信されたパケットを転送するかどうかを示します。この機能を使用するには、PC 音声 VLAN アクセスを有効にします。この機能を無効にすると、デスクトップベースの監視と録音が無効されます。

  この設定は有効です。

次の設定を無効にすることで、中間者攻撃（MITM）を防ぎます。一部のサードパーティ製のモニタリングおよび録音アプリケーションでは、このメカニズムを音声ストリームのキャプチャに使用します。

- **無償 ARP** — 無償 ARP 応答から、電話機が MAC アドレスを学習するかどうかを示します。

  この設定は無効です。

リバースプロキシ展開のセキュリティガイドライン

VPN を使用しないアクセスを許可するには、リバースプロキシホストにインターネットから直接アクセスできる必要があります。したがって、セキュリティはリバースプロキシ導入では非常に重要であり、ネットワークセキュリティを維持および管理するには、細心の注意が必要です。このセクションでは、リバースプロキシ導入を保護するための一連のガイドラインを提供します。

（注） 提供されるガイドラインと推奨事項は、管理者が導入を安全に行なうために必要な最小限のガイダンスとして使用することを目的としています。リバースプロキシとネットワークの導入、設定、およびセキュリティの責任は、コンタクトセンターにあります。

リバースプロキシ

通常、リバースプロキシは、インターネットからコンタクト センター ネットワークに入るすべての要求で最初のアプリケーションレベルの着陸ポイントになります。リバースプロキシには、攻撃に耐え得る高いレベルのセキュリティが必要です。次に、リバースプロキシ導入を保護するためのガイドラインを示します。

- TLS 1.2 を設定し、他の TLS プロトコルをオフにします。
- セキュアな HTTP/2 ベースのアクセスのみを許可します。
- プロキシへの予定外のアクセスが提供されないよう、プロキシのデフォルトアクセスとデフォルトルールをオフにします。
- リバースプロキシとホストシステムがセキュリティパッチを使用して最新の情報を入手し、侵害の可能性を防ぐことを確認します。
- リバースプロキシがインターネットへの直接のアウトバウンド接続を確立できないことを確認します。
- インターネットにさらされた場合、プロキシホストの安全性を確保するために、セキュリティを強化します。ベストプラクティスについては、https://www.cisecurity.org/cis-benchmarks/ を参照してください。
- リバースプロキシホストで定期的にセキュリティテストを実施し、セキュリティが侵害されていないかを確認します。

- セキュリティ上の理由から、明示的に公開されている以外のAPIパスは、設定されたルールで使用できないことを確認します。Nginx リバースプロキシが導入されている場合は、**「Nginx Techzone」の項目**にあるNginxルールを参照して、各Finesse、IdS、およびCUICサーバに対して明示的に開いているパスを見つけることができます。
- セキュリティの観点からキャッシュが重要なのは、ほとんどの静的リソースは保護されていないためです。Finesseサーバ上でこれらのリソースをキャッシュすることで、簡易DoS攻撃を回避できます。ただし、リソースが最新の動作を行なえるよう、Finesse、IdS、およびCUIC サーバでリソースを定期的に検証する必要があります。
- HOSTヘッダーを検証して、目的のドメインだけがクライアントによってアクセスされるのを確認します。
- 必要な数のクライアントに対応するドメインごとに、Finesse、IdS、およびCUICサーバのWebsocket 接続を調整します。
- ベストプラクティスは、更新されたパッチと設定変更で、リバースプロキシのセキュリティが強化された金色のイメージを維持することです。これらの金色のイメージからインストールすると、すべてのリバース プロキシ インスタンスに一貫性があり、可能な限り安全になります。

（注） シスコは、Nginx のリバースプロキシに関するセキュアな設定ガイドラインを **「Nginx Techzone」の項目**で説明しています。

非武装地帯のセキュリティ

ネットワークとホストのセキュリティを更新するための継続的なプロセスと関連する取り組みがない場合は、リバースプロキシの導入では、セキュリティの強化を維持できません。DMZがセキュアな環境を確保するための重要な点は次のとおりです。

- （複数のインターフェイスを備える単一のファイアウォールではなく）デュアルファイアウォールを使用して、DMZ と内部ネットワークを分離することを検討してください。
- 内部ファイアウォールでルールを設定し、DMZ から発生した要求が、リバースプロキシで設定されているホスト以外のホストに到達しないことを確認します。
- DMZ が、ルーティングとセキュリティポリシーが分離された内部ネットワークから分離されている必要があります。
- リバースプロキシ導入のセキュリティは、構成とソフトウェアを更新し続けるプロセスによって異なります。

レート制限

Finesse、IdS、およびCUICは、DoS攻撃から保護するためにホストレベルのファイアウォールルールに依存します。これらのコンポーネントでリバースプロキシホストが設定されている場合、設定されたリバースプロキシホストは、すべてのホストレベルのレート制限ルールから

免除されます。これは、プロキシに接続された複数のクライアントにサービスを提供するプロキシの必須のスループットをサポートするためにあります。したがって、逆プロキシを介してホストにルーティングされるトラフィックが個々の IP ごとに規制対象になじむよう、パケットレートの制限とレート制限要求（使用可能な場合）を適用する必要があります。これにより、リバースプロキシとホストの可用性が向上します。

（注） ネットワークを DMZ に接続する ISP ルータでは、一般的なネットワークパケットレートの制限を課すことを検討してください。周囲のルータにレート制限を実装すると、ISP リンクを飽和状態にすることを目的とした DoS 攻撃には効果的ではありません。

レートの制限の計算の詳細については、『*Cisco Unified Contact Center Enterprise Features Guide*』の「プロキシの規模とハードウェアの検討」セクション、およびNginx固有の情報については**「Nginx Techzone」の項目**を参照してください。

ネットワーク セキュリティ デバイス

DMZ に入るトラフィックに対してセキュリティを強化するために、この侵入防御システム（IPS）機能を組み込むネットワーク セキュリティ デバイスを導入する必要があります。これらは、プロキシまたはファイアウォールが効果的に検出または防止する機能を備えていないクラス全体の攻撃を防ぐためのデバイスです。IPS デバイスの導入中は、分散型サービス妨害（DDoS）署名を検出できるデバイスを導入し、DDoS 攻撃から保護します。

Web アプリケーションのファイアウォール

リバースプロキシ展開に対してより高いセキュリティ層を提供する Web Application Firewall（WAF）を導入すると良いでしょう。WAF デバイスは、セキュリティチェックをアプリケーション層に拡張します。これは、Web アプリケーション トラフィックでスクリプト、ヘッダー、Cookie、HTTP メソッドなどについて検査し、既知の脆弱性や、不正なトラフィックをブロックするループホールを見つけた場合に実現します。これにより、Webアプリケーションに固有の脆弱性を利用する複雑なサイバー攻撃が回避されます。IPS と WAF の機能を統合するデバイスや、上述のすべての機能を提供するクラウドサービスを使用するデバイスを用意することができます。

推奨される DDoS 保護

複数のクライアントを使用してDoS攻撃を開始することでレート制限を超える複雑な攻撃は、DDoS 攻撃と呼ばれます。個々のシステムが、DDoS 攻撃を検出したり、適切に反応したりできない場合が多く発生します。このような攻撃を回避するには、適切なレート制限を適用することによってトラフィックが規制されていることを確認します。

DDoS 攻撃を処理する最も効果的な方法の 1 つは、コンテンツ配信ネットワーク（CDN）を利用することによって、ほとんどの攻撃に対して高いレベルの保護を提供し、これらの総当たり攻撃の衝撃を吸収することです。DDoS 署名を検出できる IPS デバイス、ルータ、またはファイアウォールを組み込むことも、このような攻撃を防ぐのに役立ちます。

Java のアップグレード

Unified CCE は、インストールおよびアップグレード中に、基本として必要な Java バージョンをインストールします。

次のように、コンタクトセンターに Java の更新を適用できます。

- 最新の 32 ビット Java 8 マイナーバージョンの Java アップデートを適用します。

  最新の Java サポート情報については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「Contact Center Enterprise 互換性マトリクス」を参照してください。

  OpenJDK の Java の更新は OpenLogic Web サイトからダウンロードおよびインストールできます。

- Windows CCE_JAVA_HOME環境変数を変更し、変更された場合は、新しい OpenJDKJava ランタイム環境（JRE）の場所をポイントします。

Tomcat ユーティリティのアップグレード

オプションの Cisco アップグレード Tomcat ユーティリティを使用して、次のことを実行します。

- Tomcat をバージョン 9.0 ビルドリリースにアップグレードします（つまり、バージョン 9.0 ビルドリリースのみがこのツールで動作します）。最新のセキュリティ修正に対応するために、Tomcat リリース 9.0 の新しいビルドへのアップグレードを選択することができます。

  Tomcat では、メジャー.マイナー.ビルドというリリース番号のスキームが使用されます。たとえば、9.0.21 から 9.0.22 にアップグレードできます。このツールは、メジャーバージョンまたはマイナーバージョンのアップグレードには使用できません。

- 最近インストールした Tomcat が問題の原因である場合は、このユーティリティを使用して以前のバージョンをインストールします。

ツールを使用する前に:

- Tomcat インストーラー（apache-tomcat-version.exe）を Tomcat Web サイトからダウンロードします： http://archive.apache.org/dist/tomcat/tomcat-9/。インストーラーを Unified CCE コンポーネント VM にコピーします。C:\UpgradeTomcatTool など。

- ユーティリティ zip ファイルをダウンロードし、解凍し、バッチファイルを実行して Tomcat をアップグレードします。

  ダウンロード リンク: https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(1)

- これらのディレクトリ内のサイズの大きいログファイルを削除またはバックアップして、アップグレード時間を短縮します：

  c:\icm\tomcat\logs
  c:\icm\debug.txt

Tomcat のインストール

各ステップの結果の詳細については、以下を参照してくださ
い。/UpgradeTomcatResults/UpgradeTomcat.log ファイル。

（注） Tomcat ユーティリティを使用する前に、VM 上の Unified CCE サービスを停止します。

手順

ステップ 1 コマンドラインから、アップグレードした Tomcat ユーティリティをコピーしたディレクトリに移動します。

ステップ 2 ツールを実行するには、次のコマンドを入力します：**tomcatutility.bat**。

ステップ 3 プロンプトが表示されたら、使用する Tomcat のインストーラバージョンの完全なパス名を入力します。

次に例を示します。

```
c:\tomcatInstaller\apache-tomcat-9.0.21.exe
```

ステップ 4 プロンプトが表示されたら、**[はい（yes）]** を入力してインストールを続行します。

ステップ 5 すべての Unified CCE コンポーネント VM に対して、これらの手順を繰り返します。

Microsoft セキュリティの更新

サードパーティベンダーからセキュリティおよびソフトウェアの更新パッチを自動的に適用すると、いくつかのリスクがあります。機能の微妙な変化やコードの層が追加されている場合、Cisco Contact Center 製品の全体的なパフォーマンスが変化する可能性があります。

Microsoftがリリースしたすべてのセキュリティパッチを評価し、環境に適していると判断したパッチをインストールします。Microsoft Windows アップデートを自動的に有効にしないでください。更新スケジュールが、他のUnified ICM/Unified CCEアクティビティと競合する可能性があります。Microsoft Software Update Service または同様のパッチ管理製品を使用して、重大かつ重要なセキュリティパッチを選択して適用検討してください。これらの更新を適用する時期と方法については、Microsoft のガイドラインに従ってください。

（注） Microsoft for Windows、IIS、および SQL によってリリースされた重大なセキュリティパッチまたは累積アップデートのセキュリティリスクを評価します。サイトに必要と思われる重大なセキュリティパッチまたは累積アップデートを適用します。

詳細については、https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_bulletins_list.html にある『サードパーティ製のソフトウェアおよびセキュリティ アップデートを使用する場合の *Cisco Customer Contact* ソフトウェア ポリシー』を参照してください。

Microsoft Internet Information Server（IIS）

インターネット スクリプト エディタには、Internet Information Server（IIS）が必要です。ディストリビュータを除く他のノードでサービスを無効にします。ソリューションのマルチメディア設定にはいくつかの例外があります。その場合は、製品のマニュアルとシステム要件に従ってください。

Active Directory の展開

この項では、Active Directory の展開トポロジについて説明します。Active Directory（AD）展開ガイダンスの詳細は、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html の *Cisco Unified ICM/Contact Center Enterprise* ステージング ガイド を参照してください。

専用の Windows Active Directory ドメインにソリューションを展開できますが、要件ではありません。代わりに、組織単位を使用してセキュリティの基本理念を展開できます。これは AD と密接に統合し、セキュリティ委任の権限を行使することで、企業の AD ディレクトリは、アプリケーションサーバ（ドメインメンバーシップ用）、ユーザおよびサービスのアカウント、およびグループを収容するのに使用できます。

グローバル カタログの要件

Contact Center Enterprise ソリューションは、Active Directory のグローバルカタログを使用します。Unified CCE Hosts が格納されている AD フォレスト内のすべてのドメインは、そのドメインのグローバルカタログを公開する必要があります。これには、ソリューションが通信を行う認証、ユーザルックアップ、グループ検索などのすべてのドメインが含まれます。

（注） これは、フォレスト間の操作を意味するものではありません。フォレスト間操作はサポートされていません。

Active Directory サイトトポロジ

地理的に分散された Contact Center Enterprise ソリューションでは、各サイトで冗長ドメインコントローラを配置します。各サイトでグローバルカタログを確立し、サイト間複製接続を適切に構成します。Contact Center Enterprise ソリューションは、サイト内の Active Directory サーバと通信します。これには、Microsoft のガイドラインに従って適切に実装されたサイトトポロジが必要です。

組織

アプリケーションによって作成された OU

ソリューションソフトウェアをインストールする場合、VM がメンバーである AD ドメインはネイティブモードである必要があります。インストールすると、ソリューションに複数の OU オブジェクト、コンテナ、ユーザ、およびグループが追加されます。これらのオブジェクトをインストールするには、AD の組織単位に対する代理制御が必要です。ドメイン階層の任意の場所に OU を配置します。AD 管理者は、Contact Center Enterprise ソリューション OU 階層をどの程度深くネストして作成し、データを入力するかを決定します。

（注） 作成されるグループはすべてドメイン ローカル セキュリティ グループとなり、ユーザアカウントはすべてドメインアカウントとなります。サービス ログオン ドメイン アカウントは、アプリケーションサーバのローカル管理者のグループに追加されます。

Contact Center Enterprise のインストールによって、Domain Manager ツールと統合されます。このツールは OU 階層およびソフトウェアが必要とするオブジェクトを事前インストールする際にスタンドアロンで使用できます。また、設定プログラムが呼び出され、AD で同じオブジェクトを作成するときにも使用できます。AD/OU は、実行中の VM がメンバであるドメイン、または信頼できるドメイン上に作成できます。

Active Directory 管理者が作成した OU

管理者は、特定の AD オブジェクトを作成できます。主な例は、Unified CCE サーバの OU コンテナです。この OU コンテナは、特定のドメインのメンバーである VM を含めるよう手動で追加されます。ドメインに参加したら、この OU にこれら VM を移動します。この分離は、サーバを管理できる人とできない人（制御の分離）を制御します。最も重要なのは、分離が、OU 内のアプリケーションサーバが継承できる、または継承できない AD ドメイン セキュリティ ポリシーを制御する点です。

関連トピック

Windows Server の強化

ネットワークアクセス保護

ネットワークアクセス保護（NAP）は、Windows Server に導入されたプラットフォームとソリューションです。NAPは、クライアントコンピュータのシステム正常性ポリシーへの準拠に基づいてネットワークリソースへのアクセスを制御することで、ネットワークの全体的な整合性を維持するのに役立ちます。

NAP サーバは、システムの正常性ポリシーを使用してクライアントの正常性を検証します。

NAP クライアントのプラットフォーム要件の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「互換性マトリクス」を参照してください。

ネットワークポリシーサーバ

Unified CCE で承認されたソフトウェア以外の目的で Unified CCE サーバを使用しないでください。Unified CCE VM 上では、ネットワークポリシーサーバを実行しないでください。

Unified CCE サーバと NAP

NAP は、いくつかの異なる方法で使用できます。ユーザが Unified CCE で使用を検討できる導入オプションの一部を以下に示します。

- 限定されたアクセス環境を使用する Unified CCE サーバ：**サポートされません**

  警告 このモデルでは、Unified CCE サーバが準拠しなくなると、アクセスできなくなります。このアクセス不能により、マシンが再度準拠するまで、コールセンター全体がダウンします。

- Unified CCE サーバは、モニタリング専用環境を使用します。このモードは、Unified CCE サーバの正常性ステータスを追跡するために便利なものです。
- 正常性の検証から免除される Unified CCE サーバ：このモードでは、Unified CCE サーバは NAP 環境で動作しますが、ネットワークからアクセスできなくなります。Unified CCE サーバの正常性の状態は、他の Unified CCE サーバとの間の通信には影響しません。

WMI サービスの強化

Windows Management Instrumentation（WMI）は、Windows システムの管理に使用されます。WMI セキュリティは、Windows オペレーティングシステムに組み込まれたセキュリティサブシステムの拡張です。WMI セキュリティには、WMI 名前空間レベルのセキュリティ、Distributed COM（DCOM）セキュリティ、標準 Windows OS セキュリティが含まれます。

WMI ネームスペースレベルのセキュリティ

名前空間レベルのセキュリティを構成するには、次の手順を実行します。

手順

ステップ 1 `%SYSTEMROOT%\System32\Wmimgmt.msc MMC` コントロールを起動します。

ステップ 2 **[WMI 制御（WMI Control）]** アイコンを右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 3 **[セキュリティ（Security）]** プロパティのページを選択します。

ステップ 4 ルートフォルダを選択し、**[セキュリティ（Security）]** ボタンをクリックします。

ステップ 5 選択リストから全員を削除し、**[OK]** ボタンをクリックします。

<machine>\Administrators にのみすべての権限を与えます。

その他の詳細なセキュリティに関する検討事項

WMI サービスは、デフォルトで**[手動（Manual）]**のスタートアップに設定されています。サードパーティ管理エージェントは、これらのサービスを使用してシステムデータをキャプチャします。必要ではない場合、WMI サービスは無効にしないでください。

スクリプト環境と一致する方法で DCOM セキュリティの設定を実行します。DCOM セキュリティの使用の詳細については、この WMI セキュリティマニュアルを参照してください。リモートの WMI 接続のセキュリティ保護の詳細については、Microsoft Developer Network の「http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx」の項目を参照してください。

SNMP の強化

インストール、地域の名前、ユーザ名、および宛先の設定の詳細については、 *Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド を参照してください。

SNMP 管理機能には Microsoft の管理およびモニタリングツールのサブコンポーネントが必要ですが、Web セットアップツールでは、Microsoft ネイティブ SNMP サービスが無効になります。より安全なエージェント インフラストラクチャが、ネイティブの Microsoft ネイティブ SNMP サービスに置き換わります。Microsoft SNMP サービスを再び有効にしないでください。シスコがインストールした SNMP エージェントと競合する可能性があります。

Microsoft SNMP トラップ サービスを明示的に無効にします。コンタクトセンターサーバ上の SNMP トラップを収集するために管理ソフトウェアを実行しないでください。この制限により、Microsoft SNMP トラップサービスは不要になります。

SNMP プロトコルのバージョン 1 と 2c は、バージョン 3 よりも安全ではありません。SNMP バージョン3は、セキュリティの大幅なステップフォワードを特長とします。企業のファイアウォールの背後にある内部ネットワーク上にあるコンタクトセンターホストの場合は、次の設定を適用して SNMP の管理性を強化します。

1. 大文字と小文字を組み合わせて、SNMP v1/v2c コミュニティストリングまたは SNMP v3 ユーザ名を作成します。共通の「パブリック」および「プライベート」なコミュニティストリングを使用しないでください。推測が難しい名前を作成します。
2. SNMP v3 の使用を強く推奨します。各 SNMP v3 ユーザ名の認証は常に有効にします。プライバシープロトコルの使用も推奨されます。
3. SNMP 管理可能なデバイスへの接続を許可されるホストの数を制限します。
4. SNMP 管理アプリケーションを実行しているホストからの SNMP 要求のみを受け入れる管理可能デバイスで、コミュニティストリングとユーザ名を設定します。（この設定は、コミュニティストリングとユーザ名を定義する際に、SNMP エージェント設定ツールで行います）
5. 認証失敗に対する SNMP トラップの送信を有効にします。これらのトラップは、攻撃者が、コミュニティストリングやユーザ名を「推測」しようとしていることをアラートします。

SNMPの管理可能性はコンタクトセンターサーバにインストールされ、デフォルトで実行されています。ただし、セキュリティ上の理由により、前の設定手順が完了するまでSNMPアクセスは拒否されます。

セキュリティを強化するには、SNMP 管理ステーションと SNMP エージェント間の SNMP トラフィックに IPSec フィルタと IPSec ポリシーを設定します。フィルタとポリシーの設定方法に関する Microsoft の指示に従います。SNMP トラフィックの IPSec ポリシーの詳細については、Microsoft TechNet の項目を参照してください。

電話ハッカーの侵入阻止

通信業界では、料金の不正利用が深刻な問題です。電気通信技術の不正使用は企業にコストがかかる可能性があるため、電気通信管理者は、不正な使用を防ぐために必要な予防措置を取る必要があります。Unified CCE 環境では、Unified CM システムをロックダウンする方法と、料金の不正利用を軽減する方法について Cisco.com のリソースで説明しています。

Unified ICM では、Unified ICM スクリプトのラベルノードでダイナミックラベルを使用する場合が主な懸念事項です。ダイナミックラベルを、発信者が入力した情報（外部スクリプトの実行など）から作成した場合、次の形式のラベルを作成できます。

- 9.....
- 9011....
- さらに同様のパターン

これらのラベルは、コールを外部回線にも、国際番号にも送信できます。ルーティングクライアントで設定された一部のダイヤルプランでは、このような番号を通過できます。顧客がこのようなラベルを使用しない場合は、Unified ICM スクリプトで有効なラベルを使用する前にチェックする必要があります。

簡単な例は、「相手の内線が分かっている場合は、入力してください」と発信者に促す ICM スクリプトです。スクリプトは、ダイナミックラベルノードにブラインドで入力された数字を使用します。このスクリプトは、どこからでもコールを転送する場合があります。この動作が不要な場合は、Unified ICM ルーティングスクリプトまたはルーティングクライアントのダイヤルプランのどちらかをチェックして、無効な番号を禁止する必要があります。

Unified ICM スクリプトチェックの例は、次のような式を使用する 「If」 ノードです。

```
substr (Call.CallerEnteredDigits, 1, 1) = "9"
```

このノードの True ブランチはブランチバックして、発信者にもう一度尋ねます。False ブランチを使用すると、コールを続行できます。このケースは一例です。各顧客は、それぞれの環境に基づいて、何を許可し、許可しないのかを決定する必要があります。

Unified ICM は通常、コールを任意の電話番号に転送しません。番号は、法律上の宛先として明示的に設定されている必要があります。また、Unified ICM ルーティングスクリプトのロジックで、スクリプト変数からコールを電話番号に転送できます。スクリプトを作成して、発信者が一連の数字を入力し、スクリプトが宛先の電話番号として扱い、ルーティングクライアントに対してその番号にコールを転送する必要があります。要求した宛先の電話番号が適正か確認するために、このようなスクリプトにロジックを追加します。

サポートされているコンテンツ セキュリティ ポリシー ディレクティブ

コンテンツ-セキュリティ ポリシー ディレクティブ

コンテンツ セキュリティ ポリシー（CSP）のディレクティブを使用すると、Web アプリケーションがリソースがロードされている場所を定義することで、XSS 攻撃のリスクを軽減できます。

ブラウザが CSP ディレクティブで指定された場所以外の場所からデータを読み込むのを防ぐため、ヘッダーには CSP ディレクティブが使用されます。

Websetup および **Diagnostic Portico** でサポートされるコンテンツ セキュリティ ポリシー ディレクティブ

CSP directive-name	説明	directive-value
base-uri	このディレクティブは、以下で使用できるURLを制限します。 <base> 追加します。 この値が存在しない場合、任意のURLが許可されます。 このディレクティブが指定しない場合、ユーザエージェントは次の値を使用します。 <base> 追加します。	'self'
frame-ancestors	このディレクティブは、<frame> <iframe> <object> <embed><applet> を使用してリソースを埋め込む有効なソースを定義します。	'self'
default-src	default-src は、JavaScript、画像、CSS、フォント、AJAXリクエスト、フレーム、HTML5メディアなどのコンテンツのロード時に使用されるデフォルトポリシーです。	**Diagnostic Portico** の場合：'self'、'unsafe-inline' および 'unsafe-eval' **Websetup** の場合：'self'

Websetup および Diagnostic Portico のコンテンツ ポリシー ヘッダーをサポートするブラウザの詳細については、http://3.%20https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP#Browser_compatibility を参照してください。

サードパーティのセキュリティプロバイダー

シスコでは 、NTLM、Kerberos V、および IPSec セキュリティプロトコルのオペレーティングシステム実装により、Unified ICM ソフトウェアを適格にしています。

シスコでは、他のサードパーティ製セキュリティプロバイダーの実装をサポートしていません。

サードパーティ管理エージェント

サーバ オペレーティング システムのインストールでは、便利なサーバ管理とモニタリングを行うエージェントがベンダーに含まれます。

このようなエージェントは有用ですが、パフォーマンスにも影響を及ぼす可能性があります。シスコは、ミッションクリティカルな Unified ICM/CCE サーバでの使用をサポートしません。

警告 このドキュメントで説明するセキュリティポリシーに従ってエージェントを設定します。ピーク時には、ポーリングまたは業務に支障を与えるスキャンを実行するのではなく、メンテナンスウィンドウ用にこれらのアクティビティのスケジュールを設定します。

（注） これらのサードパーティ管理アプリケーションの指示に従ってSNMPサービスをインストールし、サーバに提供される管理機能を活用します。SNMP を指定しない場合、企業管理アプリケーションはハードウェア事前設定アラートを受信します。Unified CCE サーバは、32 ビットの内線エージェントのみをサポートします。

関連トピック

一般的なウイルス対策ガイドライン

自己暗号化ドライブ

Unified CCE を使用すると、リアルタイムで着信データを暗号化し、発信データを復号する特別なハードウェアを備えた自己暗号化ドライブ（SED）を導入できます。データを暗号化および復号化しても、システム全体のパフォーマンスには影響を及ぼしません。

ディスク上のメディア暗号化キーは、データの暗号化と復号化を制御します。メディア暗号キーの暗号化には、セキュリティキー（キー暗号キーまたは認証パスフレーズとも呼ばれます）が使用されます。セキュリティキーは、ユーザがローカルに提供するか、KMIP サーバを使用してリモートに提供できます。ドライブをロックしている場合は、データを取得する際にセキュリティキーは必要ありません。

SED の詳細については、『***Cisco UCS C* シリーズサーバ統合管理コントローラ *CLI* 設定ガイド**』https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html を参照してください。

導入するドライブは、仮想化 Wiki で説明されているハードドライブの仕様と一致する必要があります。詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.htmlを参照してください。

内部クラウド接続 API エンドポイント

APIはシステム内部で使用され、完全に認証され、セキュリティコンプライアンスの目的で文書化されています。ただし、お客様の使用やサードパーティとの統合の目的ではサポートされません。

API の一覧を次に示します。

- https://cloudconnecthost:port/<service-name>/status?details=true

- https://cloudconnecthost:port/inventory/<end_point>
- https://cloudconnecthost:port/Get inventory list - /inventory/managedhosts
- https://cloudconnecthost:port/Update Inventory Hosts - /inventory/managedhosts/<productType>/<clusterID>
- https://cloudconnecthost:port/Delete Inventory Hosts - /inventory/managedhosts/<productType>/<clusterID>
- https://cloudconnecthost:port/Get Nodes status - /inventory/status
- https://cloudconnecthost:port/Get Node Public Key - /inventory/controlnode/key
- https://cloudconnecthost:port/Ping API : /contm/ping
- https://cloudconnecthost:port/dataconn/ccxstreamerconfig
- https://cloudconnecthost:port/dataconn/ccestreamerconfig
- https://cloudconnecthost:port/Container List API : /contm/containers
- https://cloudconnecthost:port/Get container API : /contm/containers/{id}
- https://cloudconnecthost:port/Container start API : /contm/containers/{id}/start
- https://cloudconnecthost:port/Container Stop API : /contm/containers/{id}/stop
- https://cloudconnecthost:port/cherrypoint/config
- https://cloudconnecthost:port/cherrypoint/surveyendpoint
- https://cloudconnecthost:port/cherrypoint/dispatchtemplates
- https://cloudconnecthost:port/cherrypoint/dispatchtemplates/{dispatchTemplateId}
- https://cloudconnecthost:port/cherrypoint/surveydispatch/
- https://cloudconnecthost:port/cherrypoint/authtoken
- https://cloudconnecthost:port/cherrypoint/questionnaires
- https://cloudconnecthost:port/cherrypoint/questionnaires/v2
- https://cloudconnecthost:port/cherrypoint/questionnaires/v2/{QuestionnaireName}
- https://cloudconnecthost:port/cloudconnectmgmt/config
- https://cloudconnecthost:port/cloudconnectmgmt/config?details=true
- https://cloudconnecthost:port/cloudconnectmgmt/status
- https://cloudconnecthost:port/cloudconnectmgmt/notify
- https://cloudconnecthost:port/cloudconnectmgmt/token?scopes=scope1,scope2
- https://cloudconnecthost:port/cloudconnectmgmt/token
- https://cloudconnecthost:port/dataconn/status
- https://cloudconnecthost:port/dataconn/maintenance
- https://cloudconnecthost:port/dataconn/ccxstreamerconfig

- https://cloudconnecthost:port/dataconn/ccestreamerconfig

内部 CCE API エンドポイント

コンタクトセンター展開用の Unified CCE、Packaged CCE、HCS に適用可能な内部 API を次に示します。これらの API は、顧客の使用またはサードパーティとの統合の目的でサポートされていません。

- `/unifiedconfig/config/activedirectorydomain/`

  システムで使用可能な Active Directory ドメインを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/deployment`

  アプリケーションの現在の導入タイプを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/redirect/`

  要求を他のソリューション コンポーネントにリダイレクトするプロキシ API として使用され、`GET` メソッドと `POST` メソッドの両方をサポートします（この API は PCCE 導入にのみ適用されます）。

- `/unifiedconfig/config/downloadablefiles/`

  プライマリ AW から path param で指定されている IVR アプリケーションファイルをダウンロードするには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/smartlicense/sync/`

  スマートライセンス情報、ライセンス付与、およびサーバビーンをデータベース内のエントリと比較するには、`GET` メソッドのみサポートします。

- `/unifiedconfig/config/smartlicense/status`

  スマート ライセンス サーバのステータスを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/useridentity/authorization/migration`

  ユーザが Unified CCE to Packaged CCE 移行ツールを実行できるアクセシビリティを確認するには、`GET` メソッドのみをサポートします。