

Expressway 15.5.20のアップグレードチェックリスト

内容

[概要](#)

[使用するコンポーネント](#)

[アップグレード前](#)

[証明書の読み方](#)

[メンテナンスウィンドウの前に行う作業](#)

[アップグレードが失敗した場合](#)

[準備状況の確認でアップグレードが停止しました](#)

[ノード起動後のアラーム](#)

[管理者がサインインできません](#)

[証明書またはピアIDの障害](#)

[アップグレード中またはアップグレード直後のクラスタアラーム](#)

[ノードが起動した後のサインインの問題](#)

[TACケースが必要な場合に収集する証拠](#)

[アップグレード後](#)

[すべてのノード](#)

[クラスタのみ](#)

[使用中のサービスのチェック](#)

概要

このドキュメントでは、X15.5.20セキュリティ強化アップグレード用にExpresswayを準備する方法について説明します。各前提条件と、その修正方法について説明します。

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

アップグレード前



注意：すべてのピアが準備状況のチェックに合格するまで、クラスタのアップグレードを開始しないでください。TLS検証を適用に設定し、クラスタが正常であることを確認します。IPアドレスとFQDNの混合ではなく、1つのピアID形式を使用します。各サーバ証

明書には、SAN、またはSANが空の場合にのみCNにノードのFQDNが含まれている必要があります。CSRの作成にOpenSSLを使用した場合、空のSANが発生する可能性があります。チェックに失敗すると、既存のクラスタ設定を変更せずにアップグレードが停止します。

検証	スタンドアロン	クラスタ	それが本当でない場合
アップグレードパスが「 付録3 」に一致する	必要	必要	X8.11.4より前では、まずX8.11.4で停止します。X12 PAKライセンスを X15.xより前のスマートライセンス に変換します。
現在のバックアップとテスト済みのロールバック計画	必要	すべてのノードで必須	ウィンドウの前にバックアップを取ります。後で工場出荷時の状態にリセットすると、設定がクリアされます。
クラスタは正常、原因不明のアラームなし、レプリケーションは同期	該当なし	必要	アップグレードする前にクラスタを修正します。ローリングアップグレードでも、通常の分割クラスタ動作が使用されます。
TLS検証が適用 され、クラスタが正常です	該当なし	アップグレードの前に必要	PermissiveをEnforcingに変更し、証明書を修正し、複製を確認します。この時間帯は検出しないでください。
すべてのピアは同じID形式を使用し、ピアリストは空ではありません	ピアIDチェックパス	必要.IPとFQDNの混在は再起動前にブロックされます	すべてのFQDNまたはすべてのIPアドレスを標準化し、変更を複製し、クラスタが正常であることを確認します。ローリングアップグレード中にフォーマットを変更しないでください。
サーバ証明書には、SAN内のシステムFQDNが含まれます。SANが空の場合にのみCN内に含まれます	アップグレードで証明書を確認する場合に必要です	必要.アップグレードが停止し、クラスタ構成は変更されない	証明書を再発行します。SANが存在する場合は、CNに依存しません。NULが埋め込まれた名前を拒否します。
ピア、RSA 2048+またはP-256+、SHA-2署名によって信頼された証明書が有効	推奨	必要	SHA-1シグニチャは、X15.2ではすでにサポートされていません 。証明書を再発行します。自己署名証明書は、すべてのピアが証明書を信頼するように明示的に設定されている場合にのみ使用できます。
TCP 4371は既知のピアからのみ許可されます。	推奨	必要	ファイアウォールを制限します。これはClusterDBに対する多層防御であり、アップグレードの代わりにはなりません。
確認された管理APIクライアント	APIを使用する場合は必須	APIを使用する場合は必須	より厳密な名前とパスワードの検証、FormPutXML書き込み時のCSRFチェック、およびオプションキーAPIの使

検証	スタンドアロン	クラスタ	それが本当でない場合
			用を想定しています。
メンテナンス時間帯には、ローリングアップグレードと短いクラスタアラームの可能性が含まれます	通常のウィンドウ	必要	クッキーの再暗号化により、クラスタ通信アラームが発生する可能性があります。自然に晴れることが期待される。

証明書の読み方

サーバ証明書をエクスポートして検査します。

- SAN内のFQDN。[リリースノート](#)には、SAN内のシステムFQDNが必要です。CNがチェックされるのは、SAN拡張が空の場合だけです。
- CNフォールバックなし。SANが存在し、一致しない場合、[CNが正しくても検証は失敗します](#)。必要なすべてのDNS名またはIPアドレスを正しいSANタイプに入力します。
- NUL文字埋め込みNULを含む証明書名は拒否されます。
- 日付。notBeforeは過去の日付であり、notAfterは未来の日付である必要があります。
- Key.RSAは少なくとも2048ビット、またはP-256以上のECキー。
- 署名.SHA-2ファミリ。X15.2以降では、[sha1WithRSAEncryption](#)と[ecdsa-with-SHA1](#)はサポートされていません。
- Issuer.SubjectとIssuerが同じ場合は、自己署名です。ピアはすでに信頼している必要があります。

メンテナンスウィンドウの前に行う作業

- このウィンドウの前に、クラスタのTLS検証を[Enforcing](#)に設定し、（パブリッシャから順に）クラスタを再起動して、クラスタが正常であることを確認します。許容モードはサポートされていません。従来のPermissive値は表示されたままでも、ClusterDB証明書信頼またはピアID検証をバイパスしません。
- ピアIDはすべてFQDNであるか、すべてIPアドレスである必要があります。ローリングアップグレードの進行中は、その形式を変更しないでください。
- 複数のエイリアスを持つ認証済みのH.323エンドポイントでは、すべてのエイリアスに対して[クレデンシャルエイリアスマップ](#)が必要であるか、サブゾーンでクレデンシャルエイリアスバインディングがオフになっている必要があります。バインドをオフにすると、セキュリティポスチャが弱くなります。
- PasswordExpiryDaysが0の場合、ローカル管理者パスワードの有効期限はオフのままです。有効にすると、時間切れはローカルの深夜0時ではなく、00:00 UTCに計算されます。
- [パスワード履歴の深さは、デフォルトで12に設定](#)されます。トレーニングの範囲は3 ~ 24です。空の管理者パスワードは拒否され、最近使用したパスワードは拒否されます。
- [LDAP管理者とロールのマッピング](#)では、グループ名の完全一致が必要です。設定済みの名前のみを含むグループ名では、ロールが付与されなくなりました。
- 新規インストール、工場出荷時設定へのリセット、または無人導入では、[工場出荷時設定の](#)

[ルートパスワード](#)を再利用できません。アップグレードを行っても、現在の管理者パスワードは消去されません。

- 読み取り専用管理者は、SAML IdP信頼を変更できなくなりました。
- STARTTLSを完了できないEメールはクリアテキストでは送信されません。
- [Smart Licensing](#)は唯一のライセンスモードです。PAKオプションキーはX14.2で削除されました。標準のExpresswayイメージでは、[2500の暗号化されたシグナリングセッション](#)が可能です。Expressway Selectは上限なしのイメージです。

アップグレードが失敗した場合

クラスタはそのままにしておきます。準備状況の確認に失敗しても、既存のクラスタ設定は変更されません。ノードを工場出荷時の状態にリセットして障害を回避しないでください。

準備状況の確認でアップグレードが停止しました

証明書、TLS検証、またはピアIDの要件が失敗すると、再起動の前にインストーラが停止します。スタンドアロンノードはピアIDチェックに合格します。

ノード起動後のアラーム

クラスタデータベースの再暗号化のバーストにより、クラスタ通信障害アラームが発生する可能性があります。終了までの時間を与えます。引き続き稼働している場合はエスカレーションします。

管理者がサインインできません

この問題は、インストールの失敗とは別に扱ってください。期限切れ、再利用、または最初のログインパスワードによってセッションがブロックされます。これは、イメージの障害を意味するものではありません。

証明書またはピアIDの障害

1. 停止したノードから完全なシステムスナップショットをダウンロードします。そのスナップショットのtmpディレクトリでinstall-errorを開きます。
2. メッセージがピアIDに関するものである場合は、IPアドレスとFQDNが混在していないか、または空のピアリストがないかを確認します。すべてのピアで1つの形式を使用し、レプリケーションを待機し、クラスタが正常であることを確認してから、再試行してください。ローリングアップグレードの途中でID形式を変更しないでください。
3. メッセージが証明書に関するものである場合は、リリースノートのルールと比較してください。システムFQDNはSAN内にあるか、またはSANが空のときにのみCN内にある必要があります。現在のSANはCNにフォールバックできません。
4. 正しいSANタイプで、必要なすべてのDNS名またはIPアドレスを使用して証明書を再発行します。埋め込みNULを含む名前を拒否します。
5. 新しい証明書が日付に準拠し、RSA 2048+またはP-256+で信頼され、SHA-2で署名されて

いることを確認します。ケースに秘密鍵を添付しないでください。

6. TLS検証をEnforcingに設定し、クラスタが正常であることを確認して、停止したノードでアップグレードを再試行します。
7. ローリングアップグレードは、そのノードが正常な状態になった後にのみ続行します。このチェックで1つのノードが停止している間は、残りのノードをアップグレードしないでください。

アップグレード中またはアップグレード直後のクラスタアラーム

1. アップグレード自体が完了し、ノードがX15.5.20上にあることを確認します。
2. イベントログで、ClusterDBフィールドの再暗号化に関するdeveloper.upgradeメッセージを確認し、「Saving migrated data to CDB」を確認します。
3. アラームがクリアされるまで待ちます。トレーニング資料には、再暗号化が完了すると消去されると記載されています。
4. 残っている場合は、各ピアからクラスタステータス、アラーム、およびスナップショットを収集します。ケースのメモにクラスタCookieやキー情報をコピーしないでください。
5. TCP 4371と4372がピア間でのみオープンであり、相互TLSが成功することを確認します。任意の場所から4371を許可するファイアウォールは修正されません。

ノードが起動した後のサインインの問題

- Web UIがパスワードの変更にリダイレクトされます。現在のパスワードを入力する必要があります。また、新しいパスワードは異なるパスワードにする必要があります。これは、インストールまたは工場出荷時設定へのリセット後、およびローカルパスワードの有効期限が切れた後の最初のGUIログインで予期されます。
- SSHは、キーボードインタラクティブ/PAMが失敗したと通知し、シェルを開きません。期限切れのローカルパスワードを変更する必要があります。古いセッションは許可されていません。
- RESTは401を返します。期限切れのローカル管理者が必要です。イベントログに、APIレールのパスワードの不一致またはtaa-chkpasswdエラーが記録される場合があります。パスワードを変更してから、再試行してください。
- 新しいパスワードが拒否されました。履歴（デフォルトは最後の12）に含まれているか、現在の複雑度ルールに失敗しています。
- LDAP管理者は必要な役割を失いました。設定したグループを、LDAPから返された正確なグループ名と比較します。部分一致または部分文字列一致では、ロールが付与されなくなりました。読み取り専用の管理者は、SAML IdP信頼を編集できません。
- 新規インストールまたは工場出荷時の初期状態へのリセットでは、工場出荷時のデフォルトのルートパスワードはありません。デフォルトのクレデンシャルを検索したり、配布したりしないでください。アップグレードしても、現在の管理者パスワードはクリアされません。



注意：工場出荷時状態へのリセットは、アップグレード/リカバリの手順ではありません。クラスタIDとクラスタCookieを削除します。クラスタリング解除が行われた後のシステムによるリセットや、一貫性のないクラスタデータベースでは、IPアドレスと管理者パスワードおよびルートパスワードが保持され、他の設定とログがクリアされて、ノード

が一時証明書に戻されます。リリースノートで呼び出された場合、およびバックアップが存在する場合にのみ使用します。

TACケースが必要な場合に収集する証拠

1. 各ノードのソフトウェアバージョンとロール、および停止したノード。
2. 障害が発生したノードからの完全なシステムスナップショット (tmp/install-errorを含む) 。
3. サーバー証明書テキスト(openssl x509 -text -noout)。 秘密キーがありません。
4. クラスタステータス、アラーム、およびxConfiguration Cluster TlsVerifyでPermissiveとEnforceのどちらが表示されるか。
5. アップグレードのイベントログ行、および関連する場合はsshdまたはhttpd認証の失敗。パスワードとCookieを修正します。
6. ローカル、LDAP、SAMLのどの管理者を使用している、Smart Licensingと任意のAPIの自動化を使用できます。

アップグレード後

すべてのノード

1. バージョンはX15.5.20ビルドを対象としています。
2. ノードは管理アドレスで到達可能で、Web UIがロードされます。
3. 新しいハードウェア、ディスク、またはアプリケーションアラームは発生しません。(クラスタ通信アラームは、再暗号化後にクリアされます) 。
4. クラスタが安定した後、新しいバックアップが作成されます。

クラスタのみ

1. クラスタ内のすべてのピアが稼働しており、レプリケーションは正常です。
2. ピアはTCP 4371および4372で相互TLSと通信します (有効なクライアント証明書のない接続は失敗します) 。
3. クラスタTlsVerifyが適用されています。

Permissiveはサポートされていません。従来のPermissive値は引き続き表示できますが、検証をバイパスしません。Enforcingを設定し、クラスタが正常であることを確認します。

4. ファイアウォールは、ピアアドレスからのTCP 4371のみを引き続き許可します。
5. アップロードしたログまたはスナップショットのメモに、クラスターCookieまたは診断シークレットが表示されません。

使用中のサービスのチェック

使用している場合	見た目の良さ	失敗した場合
ローカル管理者	GUI、SSH、およびAPIは、現在のパスワードを受け入れ	有効期限が00:00 UTCであり、新しいパスワードが履歴ウィンドウの外にあることを確認します。

使用している場合	見た目の良さ	失敗した場合
	ます。期限切れのアカウントはパスワード変更にプッシュされるか、HTTP 401を受信します。	
LDAP管理者	管理者は、LDAPグループ名が設定済みグループと正確に一致する場合にのみサインインします。	ディレクトリグループをExpresswayグループと比較します。ログインを強制するために一致を拡張しないでください。
SIPまたはB2Bコール	テストコールは両方向で接続します。	通話履歴とスナップショットを収集します。
認証されたH.323登録	エンドポイントは、H.323 IDやE.164番号など、使用するすべてのエイリアスに登録されます。	エイリアスごとにクレデンシャルエイリアスマップを追加します。 リリースノート では、パターンタイプがExactのxConfiguration Registration CredentialAliasMapを使用しています。サブゾーンでCredentialAliasBindingをオフにすると、登録も復元され、セキュリティポスチャが弱体化します。H.323自体は削除されません。
MRAまたはデバイスは登録	既知のエンドポイントが登録され、コールが発信されます。UCクライアント証明書SANは、特定のDNS名またはIPアドレスであり、過度に広い値や不正な値ではありません。	証明書、トラバーサルクレデンシャル、およびDNSを、アップグレード前のバックアップと比較します。SANの範囲が広すぎる証明書を再発行します。
電子メールアラート	テストメッセージは、STARTTLSを使用してノードから送信されます。	STARTTLSが完了できない場合、配信はクローズされません。メールサーバの信頼またはTLSを修正します。クリアテキストのフォールバックを想定しないでください。
Smart Licensing	登録と許可はWeb UIと一致します。標準イメージは 2500暗号化シグナリングセッション 内に残るか、ノードはExpressway Selectです。	トランスポートとCSSMを確認します。CSSMの「エクスポート制御機能を許可する」チェックボックスは、Expresswayには適用されません。トークンを取り消して製品インスタンスを削除すると、ノードの登録が解除されます。オプションキーは回避策ではありません。
RESTまたは設定スクリプト	アカウント名は、新しい長さで文字数の制限に一致します。設定の書き込みには、GUIで使用するCSRF保護が含まれます。	出荷されているAPIスキーマに対してクライアントを更新します。削除された/provisioning/optionkeyコールは失敗することが予想されます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。