

サポート バンドル Identity Services Engine を on Cisco 集めて下さい

目次

[はじめに](#)

[サポート バンドル ISE を on Cisco 集めて下さい](#)

[ステップ 1. ISE コンポーネントのためのイネーブル デバッグ](#)

[ステップ 2.問題を作り直して下さい](#)

[ステップ 3.ディセーブル デバッグ](#)

[ステップ 4.サポート バンドルを集めて下さい](#)

概要

この資料 describes Cisco Identity Services Engine (ISE) からサポート バンドルを集める方法を。サポート バンドルは ISE を解決するための鍵情報 necessary が含まれています。サポート バンドルの収集は CLI および GUI によって両方達成されるかもしれません。

サポート バンドル ISE を on Cisco 集めて下さい

ステップ 1. ISE コンポーネントのためのイネーブル デバッグ

ISE のさまざまな問題はトラブルシューティングのためにログの異なるセットを必要とします。必要なデバッグの詳細なリストは TAC エンジニアによって提供する必要があります。この資料は ISE を解決するために使用されるもっとも一般的な問題およびデバッグについての情報を提供したものです。このリストの目的はケース解決を高速化し、TAC ケースの最初のトラブルシューティングの間に詳細を提供するかもしれないログの収集と助けることです。

TAC エンジニアが要求するデバッグのリストはこのリスト上の優先順位を常に奪取 する必要があります。

問題	コンポーネント名
	ランタイム AAA (デバッグ)
	ランタイム構成 (デバッグ)
認証/許可	ランタイム ロギング (デバッグ)
	epm-pdp (デバッグ)
	prrt-JNI (デバッグ)
Active Directory	Active Directory (トレース)
	識別ストア AD (デバッグ)
	ゲスト Admin アクセス (デバッグ)
	ゲスト Admin (デバッグ)
ゲスト ポータル	guestaccess (デバッグ)
	ポータル (デバッグ)
	門脈セッション マネージャ (デバッグ)
	門脈 Web 処理 (デバッグ)
スポンサー ポータル	sponsorportal (デバッグ)
	ポータル (デバッグ)

	門脈セッション マネージャ (デバッグ) 門脈 Web 処理 (デバッグ)
SMS、電子メール通知	ゲストまたはスポンサー ポータル デバッグ (上記参照) NotificationTracker (デバッグ) パケットキャプチャ (デバッグ)
MDM	mdmportal (トレース) 外部mdm (トレース) パケットキャプチャ (デバッグ) クライアントwebapp (デバッグ)
クライアント プロビジョニング	提供 (デバッグ) ポータル (デバッグ) 門脈セッション マネージャ (デバッグ) 門脈 Web 処理 (デバッグ) クライアントwebapp (デバッグ) certprovisioningportal (デバッグ)
BYOD	oscp 応答側 (デバッグ) 提供 (デバッグ) ポータル (デバッグ) 門脈セッション マネージャ (デバッグ) 門脈 Web 処理 (デバッグ)
プロファイリング	プロファイラー (デバッグ) プロファイラー (デバッグ)
エンドポイント 関連 問題	ers (デバッグ) epm papapi.service (デバッグ) mydevices (デバッグ)
ポスチャ	ポスチャ (デバッグ) クライアントwebapp (デバッグ) 提供 (デバッグ)
複製/同期	複製配備 (デバッグ) Replication-JGroup (デバッグ) ReplicationTracker (デバッグ) cpm mnt (デバッグ)
モニタリング/ログ	Cisco mnt (デバッグ) VC (デバッグ) VC db (デバッグ) 報告して下さい (デバッグ)

Administration > システムロギング > デバッグ ログ 設定にナビゲートし、デバッグが有効にする必要がある ISE ノードを選択して下さい:

水平なデバッグするために適切なコンポーネント名 (レッド) および増加ログを選択して下さい (オレンジ)

Node List > akotwica-ise241.example.com
Debug Level Configuration

ボタンを確認して下さい (紫色) 『SAVE』 をクリック することクリックして変更を。操作の上でデバッグ リストからの各デバッグのために繰り返される必要があります (この資料でまたは TAC エンジニアによって提供されて)。

ステップ 2.問題を作り直して下さい

すべての必要なデバッグが有効になるとき、ログを生成するために問題を作り直して下さい。問題が手動で引き起こすことができない場合次の発生を待つはずでず。デバッグが有効になった前に問題が発生したらそこにトラブルシューティングのための情報が十分あるかもしれません。理想的には、サポートバンドルは問題が発生した直後に集める必要があります。ログ分析のために必要とされる注補助情報:

- タイムスタンプはの作り直します
- MAC アドレスのようなイベントのためのあらゆる unique ID、IP アドレス、ユーザ名、セッションID (、通常 MAC/IP + ユーザ名は状況によってです十分は決まります)

ステップ 3.ディセーブル デバッグ

問題が作り直される直後に、問題のためにちょうど生成した上書きログから広範なロギングを防ぐためにデバッグを無効にして下さい。

ステップ 4. サポート バンドルを集めて下さい

記録すべきナビゲート: デバッグが有効になったところ)、オペレーション >> ダウンロード ログおよび選定された ISE ノード (1 解決します。

その各ノードの ON タブは 2 つのオプションです: サポート バンドル (レッド) またはダウンロード特定のログファイルを集めて下さい-デバッグは記録します (オレンジ)

デバッグ ログに関しては、すべての利用可能な ログファイルの詳細なリストは表示する。ファイルの名前をクリックした後それはダウンロードされます:

Debug Log Type	Log File	Description
ise-psc		Main ise debug log messages
	ise-psc.log	
	ise-psc.log.2018-08-28.1	
	ise-psc.log.2018-08-29.1	

サポート バンドルは選択したグループからのすべてのログが含まれているパッケージです。

Include full configuration database ⓘ
 Include debug logs ⓘ
 Include local logs ⓘ
 Include core files ⓘ
 Include monitoring and reporting logs ⓘ
 Include system logs ⓘ
 Include policy configuration ⓘ

- すべてのコンフィギュレーション データベースはバンドルをサポートするために完全な ISE 設定を接続します。
- デバッグ ログはそれはすべての ISE コンポーネントからのすべてのデバッグが含まれているので最も広く使われています、
- ローカル ログはログが含まれています配備でこの特定のノードのための RADIUS 認証を示す、
- コア ファイルによりサポート バンドルは育ちます場合がありますがクラッシュ トラブルシューティングの間にそれが必要となります、
- モニタリングおよびレポート ログは運用データが含まれています、
- システムログはシステム特定のログが含まれています (OS によって提供されるサービスをトラブルシューティングのために)、
- ポリシー 設定- ISE の設定されたポリシーの XML バージョン。

デバッグ ログおよびローカル ログを含むシナリオのほとんどのために、十分であって下さい。安定性およびパフォーマンス上の問題に関してはまた芯を取ればシステムログは必要です。公開鍵 暗号化だけを選択すれば TAC は Cisco プライベートキーを使用してこのバンドルを復号化できます。共有鍵はログを復号化するために必要である set password に可能にします。共有鍵の場合には、TAC エンジニアはそれにアクセスできる、従ってバンドルは on Cisco 復号化された側である場合もありますことを確認して下さい。

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ

From Date

 ⓘ (mm/dd/yyyy)

To Date

 ⓘ (mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

▼ Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

* Note: Log bundle may contain sensitive data. Ensure it is only distributed to authorized personnel.

Create Support Bundle

すべてが一定の『Create』をクリックするサポートバンドルボタンをおよびとき待つて下さい。

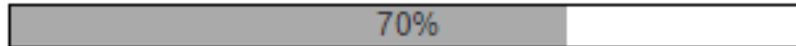
▼ Support Bundle - Status Summary

File Name: ise-support-bundle-pk-akotwica-ise241-admin-09-12-2018-10-15.tar.gpg

Start Time: Wed Sep 12 10:15:48 CEST 2018

Message: Support Bundle generation is in progress..

Progress: Copying debug logs



サポートバンドルの作成のプロセスが完了する時サポートバンドルはダウンロード可能です。
『Download』をクリックすることの後でボタンサポートバンドルはPCのlocaldiskで保存され、トラブルシューティングのためのTACにアップロードすることができます。

▼ Support Bundle - Status Summary

File Name: ise-support-bundle-pk-akotwica-ise241-admin-09-12-2018-10-15.tar.gpg

Start Time: Wed Sep 12 10:15:48 CEST 2018

Message: Support Bundle generation completed

Progress:

▼ Support Bundle - Last Generated

File Name: ise-support-bundle-pk-akotwica-ise241-admin-09-12-2018-10-15.tar.gpg

Time: Wed, 12 Sep 2018 10:24:42 CEST

Size(KB): 6689.0

Download

Delete

Webインターフェイスが available ではない場合 CLI から Support バンドルを集めることができます。これを、ログオンかコンソール公債アクセス SSH を使用してするためにおよび使用は命じます:

```
backup-logs name repository ftp {encryption-key plain key | public-key}
```

名前-あなたの名前はバンドルをサポートします

ftp - ISE で設定されるリポジトリの名前

キー-暗号化/復号化サポート バンドルに使用するキーはあります

サポート バンドルをアップロードするための公式 ツール:

<https://cway.cisco.com/csc/>

サポート バンドル ファイルの拡張を ZIP にしませんでしたり、または変更しないで下さい。それは ISE からダウンロードされたのと同じ正確な状態でアップロードする必要があります。