AsyncOS 11.1.3 for Cisco Email Security Appliances リリースノート

発行日:2019 年 7 月 8 日

目次

今回のリリースでの変更点

AsyncOS 11.1.3 の新機能

このリリースには、動作の変更と複数のバグ修正が含まれています。詳細については、動作における変更(6 ページ)および既知および修正済みの問題(18 ページ)を参照してください。

Cisco Systems, Inc.
www.cisco.com

AsyncOS 11.1.2 の新機能

機能	説明
DMARC 検証をスキップしたメッセージを処理するためのコンテンツ フィルタおよびメッセージ フィルタの設定	DMARC 検証をスキップしたメッセージに対してアクションを実行するようにアプライアンスを設定できます。 Other Header コンテンツ フィルタで次の設定を使用して、DMARC 検証をスキップしたメッセージを分類します。 • ヘッダー名を「`X-Ironport-Dmarc-Check-Result`」として追加します。 • [ヘッダー値(Header Value)] を選択して、[等しい(Equals)] を選択し、`validskip`、`invalidskip`、`temperror`、`permerror` のいずれかの値を追加します。 DMARC 検証をスキップしたメッセージの分類に使用するメッセージ フィルタ ルールの構文の例を次に示します。 `Quarantine_messages_DMARC_skip: if (header("X-Ironport-Dmarc-Check-Result") == "^validskip$") { quarantine("Policy"); }` コンテンツ フィルタとメッセージ フィルタで使用されるヘッダー値の詳細については、Cisco TAC にお問い合わせください。

AsyncOS 11.1.1 の新機能

機能	説明
偽装電子メール検出の強化	[Mail Policies] > [Address Lists] を選択して、完全な電子メール アドレスのみで構成された例外リストを作成し、偽装電子メール検出コンテンツ フィルタをバイパスすることができます。 アプライアンスで、設定済みのコンテンツフィルタから電子メール アドレスをスキップする場合、偽装電子メール検出ルールでこの例外リストを使用できます。

AsyncOS 11.1 の新機能

機能	説明
短縮 URI の URL フィルタリング サポート	短縮 URI に対して URL フィルタリングを実行するようにアプライアンスを設定し、短縮 URL から実際の URL を取得できるようになりました。元の URL の URL レピュテーション スコアに基づいて、設定済みのアクションが短縮 URL で実行されます。 短縮 URLで URL フィルタリングを有効にするには、アプライアンスが次のドメインに接続できる必要があります。 • bit.ly • tinyurl.com • ow.ly • tumblr.com • ff.im • youtu.be • tl.gd • plurk.com • url4.eu • j.mp • goo.gl • fb.me • alturl.com • wp.me • chatter.com • tiny.cc • ur.ly **（注）** ドメインのリストはクラウドで更新可能です。 アプライアンスで短縮 URL の URL フィルタリングを有効にするには、ユーザ ガイドまたはオンライン ヘルプの「Protecting Against Malicious or Undesirable URLs」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliance*』を参照してください。
添付ファイルでの URL のスキャンのサポート	メッセージの添付ファイルの URL をスキャンするようにアプライアンスを設定し、そのようなメッセージに対して設定されているアクションを実行できるようになりました。 URL レピュテーションと URL カテゴリのコンテンツおよびメッセージ フィルタを使用して、メッセージの添付ファイルの URL をスキャンできます。詳細は、ユーザ ガイドまたはオンライン ヘルプの「Using Message Filters to Enforce Email Policies」、「Content Filters」、および「Protecting Against Malicious or Undesirable URLs」の章を参照してください。

機能	説明
AMP for Endpoints コンソールの統合	アプライアンスを AMP for Endpoints コンソールと統合し、独自のブロックまたは許可ファイル SHA を追加できるようになりました。 統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。 アプライアンスを AMP for Endpoints コンソールと統合するには、ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。 [高度なマルウェアレポート（Advanced Malware Report）] ページに、AMP for Endpoints コンソールから受信したブロックファイル SHA の割合を表示する、新しいセクション [カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] が含まれるようになりました。ブロックファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションに [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 ユーザ ガイドまたはオンライン ヘルプの「File Reputation Filtering and File Analysis」の章を参照してください。
スキャン不可のメッセージの処理	次のエンジンによってスキャンされないメッセージを処理するようにアプライアンスを設定できるようになりました。 • コンテンツ スキャナ • ファイルのレピュテーションとファイルの分析サービス • URL フィルタリング このようなメッセージに対して適切なアクションを設定するには、ユーザ ガイドまたはオンライン ヘルプの「Using Message Filters to Enforce Email Policies」、「File Reputation Filtering and File Analysis」、「Protecting Against Malicious or Undesirable URLs」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

機能	説明
事前分類の有効性の改善 （Cisco AMP Threat Grid へのファイルのアップロードを減らす）	アプライアンスのファイル分析サービスは、Cisco AMP Threat Grid でサポートされているすべてのファイルの種類をサポートするようになりました。 この機能を使用して次のことができます。 • ファイル分析用の動的なコンテンツを含むファイルのみをアップロードします。これは、管理者が毎日のファイルのアップロード制限をトラッキングするのに役立ちます。 • ファイル分析のためのファイルのアップロードを減らします。 （注） プライベート クラウド ファイル分析サーバのバージョン 2.4 またはそれ以前のバージョンを使用している場合は、ファイル分析に新しいファイル タイプを有効にしないことをお勧めします。 この機能を設定するには、ユーザ ガイドまたはオンライン ヘルプの「File Reputation Filtering and File Analysis」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。 新しい判定 - ファイルの分析後に、ファイルに動的なコンテンツが存在しないときの新しい判定 [Low Risk] が導入されました。[Advanced Malware Protection] レポートの [Incoming Files Handed by AMP] セクションおよびメッセージ トラッキングで、判定の詳細を表示できます。詳細については、ユーザ ガイドの「Tracking Messages」の章を参照してください。
ファイル レトロスペクティブ アラートの改善	メッセージ受信者に配信されない、ドロップまたは隔離されたメッセージに対するレトロスペクティブ判定アラートを抑制するようにアプライアンスを設定できるようになりました。 この機能を有効にするには、「File Reputation Filtering and File Analysis」または『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
CASE の強化	スパム対策の効率性を向上させるために、アプライアンスが DMARC、SPF、DKIM 情報をコンテキスト適応スキャン エンジンに送信するようになりました。 （注） Cisco Email Security Appliance は、組織の機密データをコンテキスト適応スキャン エンジンに送信しません。
アプライアンスで有効になっているサービス エンジンのステータスの再起動と表示	CLI で `diagnostic > services` サブコマンドを使用して、以下を実行できます。 • アプライアンスで有効になっているサービス エンジンを再起動します。アプライアンスを再起動する必要はありません。 • アプライアンスで有効になっているサービス エンジンのステータスを表示します。 この機能を使用するには、ユーザ ガイドまたはオンライン ヘルプの「System Administration」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

機能	説明
メッセージ ヘッダーの優先順位の設定	メッセージ ヘッダーの優先順位を設定して、アプライアンスの受信メッセージと送信メッセージを一致させることができます。 この機能を有効にするには、ユーザ ガイドまたはオンライン ヘルプの「Mail Policies」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
ファイルのレピュテーション サービス用に APJC 地域に追加された新しいデータセンター	シスコはファイルのレピュテーション サービス用に APJC 地域に次の新しいデータセンターを追加しました。 *APJC (cloud-sa.apjc.amp.cisco.com)* 新しいファイル レピュテーション サービスを使用するように、Email Security Appliance を設定できます。詳細については、ユーザ ガイドまたはオンライン ヘルプの「File Reputation Filtering and File Analysis」の章を参照してください。

動作における変更

AsyncOS 11.1.3 の動作の変更

データ損失防止（DLP）でサポートされる文字エンコーディングの変更	データ損失防止（DLP）では、中国語、日本語、韓国語のマルチバイト プレーン テキストファイルに対して、次の文字エンコーディングがサポートされるようになりました。 • 中国語（繁体字）（Big5） • 中国語（簡体字）（GB2312） • 韓国語（KS-C-5601/EUC-KR） • 日本語（Shift-JIS（X0123）） • 日本語（EUC） ただし、データ損失防止（DLP）は、次の文字エンコーディングをサポートしません。 • 日本語（ISO-2022-JP） • 韓国語（ISO2022-KR） • 中国語（簡体字）（HZGB2312）

メールポリシー設定の変更	このリリースへのアップグレード後、アプライアンスが着信メッセージと発信メッセージのメッセージヘッダーをチェックする際の優先順位を設定できるようになりました。最初に、アプライアンスはすべてのメールポリシーで優先順位の最も高いメッセージヘッダーをチェックします。いずれのメールポリシーとも一致するヘッダーがない場合、アプライアンスはすべてのメールポリシーの優先順位リスト内の次のメッセージヘッダーを検索します。いずれのメールポリシーとも一致するメッセージヘッダーがない場合は、デフォルトのメールポリシー設定が使用されます。
Attachment File Info コンテンツ フィルタまたはメッセージ フィルタの変更	次のいずれかの条件に基づいて、アプライアンスで 'Attachment File Info' コンテンツ フィルタまたはメッセージ フィルタを設定します。 • [ファイル名(Filename)] オプションを選択して、[等しくない(Does Not Equal)]、[含まない(Does Not Contain)]、[次で終わらない(Does Not End With)]、または [始まらない(Does Not Begin)] オプションを選択し、ファイル名を入力する。 • [ファイル タイプ(File type)] オプションを選択して、[一致しない(Is not)] オプションを選択し、ドロップダウン リストからファイル タイプを選択する。 • [MIME タイプ(MIME type)] オプションを選択して、[異なる(Is Not)] オプションを選択し、MIME タイプを入力する。 アプライアンスは、上記のいずれかの条件に基づいて、添付ファイルがあるかどうかにかかわらず、メッセージに対して設定されたアクションを実行するようになりました。

AsyncOS 11.1.2 の動作の変更

USEDNS キーワードを使用した SMTP ルート設定に対する変更	このリリースより前のリリースでは、宛先ポートとしてデフォルトのポート(25)のみを使用して、USEDNS キーワードで SMTP ルートを設定することができました。 このリリースにアップグレードした後は、任意の有効な宛先ポートを使用して、USEDNS キーワードで SMTP ルートを設定できます。

AsyncOS 11.1.1 の動作の変更

デモ証明書の変更	このリリース以前は、アプライアンスが TLS 接続を有効にするデモ証明書で事前に設定されています。 このリリースにアップグレードすると、アプライアンスは TLS 接続を有効にする一意の証明書を生成します。次の設定で使用されている既存のデモ証明書は新しい証明書に置き換えられます。 • メール配信 • LDAP • ネットワーキング • URL フィルタリング • SMTP サービス
自己署名証明書の変更	このリリースより前のリリースでは、アプライアンスは SHA-1 署名ハッシュ アルゴリズムを使用して自己署名証明書を作成していました。 このリリースへのアップグレード後、アプライアンスは SHA-256 署名ハッシュ アルゴリズムを使用して自己署名証明書を作成します。
グレイメールの URL 書き換えの変更	アプライアンスでグレイメールと安全な配信停止が有効になっている場合、アプライアンスは、長さが 2000 文字未満の元の配信停止 URL のみを書き換えます。

AsyncOS 11.1 の動作の変更

コンテンツ フィルタおよびメッセージ フィルタの URL Reputation と URL Category の変更	このリリースより前のリリースでは、アプライアンスで 'URL Category' または 'URL Reputation' コンテンツ フィルタまたはメッセージ フィルタを設定した場合、アプライアンスはメッセージの本文および件名内の URL をスキャンします。 このリリースにアップグレードした後は、メッセージの本文および件名とメッセージの添付ファイル、またはその両方に含まれる URL をスキャンするようにアプライアンスを設定できます。 'URL Reputation' および 'URL Category' コンテンツ フィルタとメッセージ フィルタの条件には、次の新しいオプションが含まれます。 • [Include Attachments] - メッセージの添付ファイル内の URL をスキャンします。 • [Include Message Body and Subject] - メッセージの本文および件名内の URL をスキャンします。
S/MIME 検証の変更	Cisco E メール セキュリティ アプライアンスでは、S/MIME 証明書の検証中に送信者ドメインの認証局も検証されます。
設定ファイルの変更	Web インターフェイスまたは CLI で “plain passphrase” オプションを使用して、アプライアンスの設定ファイルを保存できなくなりました。

アップグレードの方法

リリース 11.1.3-009 へのアップグレード - MD（メンテナンス導入）

次のバージョンから、リリース 11.1.3-009 にアップグレードすることができます。

- 11.0.0-274
- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.1.0-069
- 11.1.0-086
- 11.1.0-128
- 11.1.0-131
- 11.1.0-135
- 11.1.0-140
- 11.1.0-143
- 11.1.0-404
- 11.1.0-603
- 11.1.1-042
- 11.1.2-023
- 11.1.2-509
- 11.1.2-701
- 11.1.2-802
- 11.1.3-006

リリース 11.1.2-023 へのアップグレード - MD（メンテナンス導入）

次のバージョンから、リリース 11.1.2-023 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-037
- 11.0.2-044
- 11.1.0-131
- 11.1.0-135
- 11.1.1-037
- 11.1.1-042

リリース 11.1.1-042 へのアップグレード - MD（メンテナンス導入）更新

次のバージョンから、リリース 11.1.1-042 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-037
- 11.1.0-069
- 11.1.0-072
- 11.1.0-086
- 11.1.0-131
- 11.1.0-135
- 11.1.0-140
- 11.1.0-143
- 11.1.1-030
- 11.1.1-032
- 11.1.1-037

（注） AsyncOS 11.1.1-037 を使用しているが、アプライアンスをより高いバージョンにアップグレードできない場合は、シスコ カスタマー サポートに連絡して、アプライアンスを以前の AsyncOS バージョンに戻してください。アプライアンスを以前のバージョンに戻した後、AsyncOS 11.1.1-042 にアップグレードできます。これは既知の問題です。
障害 ID：CSCvm48037

リリース 11.1.1-037 へのアップグレード - MD（メンテナンス導入）更新

次のバージョンから、リリース 11.1.1-037 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-037
- 11.1.0-069
- 11.1.0-072
- 11.1.0-131
- 11.1.0-135
- 11.1.0-140
- 11.1.0-143

リリース 11.1.1-032 へのアップグレード - MD（メンテナンス導入）

次のバージョンから、リリース 11.1.1-032 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-037
- 11.1.0-069
- 11.1.0-072
- 11.1.0-131

リリース 11.1.1-030 へのアップグレード - LD（限定的な導入）

次のバージョンから、リリース 11.1.1-030 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-037
- 11.1.0-069
- 11.1.0-072
- 11.1.0-131
- 11.1.0-135
- 11.1.0-140
- 11.1.0-143

リリース 11.1.0-131 へのアップグレード - GD（一般導入）更新

次のバージョンから、リリース 11.1.0-131 にアップグレードすることができます。

- 10.0.2-020
- 10.0.3-004
- 11.0.0-264
- 11.0.0-274
- 11.0.1-027
- 11.1.0-069
- 11.1.0-072
- 11.1.0-086
- 11.1.0-128

リリース 11.1.0-086 へのアップグレード - LD（限定的な導入）更新

次のバージョンから、リリース 11.1.0-086 にアップグレードすることができます。

- 11.1.0-069
- 11.1.0-072

リリース 11.1.0-072 へのアップグレード - LD（限定的な導入）更新

次のバージョンから、リリース 11.1.0-072 にアップグレードすることができます。

- 9.8.1-015
- 10.0.0-203
- 10.0.1-103
- 10.0.2-020
- 10.0.2-107
- 10.0.3-004
- 11.0.0-264
- 11.0.0-274
- 11.0.1-027
- 11.0.1-030
- 11.0.1-030
- 11.1.0-054
- 11.1.0-069

リリース 11.1.0-069 へのアップグレード - LD（限定的な導入）

次のバージョンから、リリース 11.1.0-069 にアップグレードすることができます。

- 10.0.3-004
- 11.0.0-274
- 11.0.1-030
- 11.0.1-027
- 11.1.0-054

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

アップグレードするには、管理者としてログインする必要があります。また、アップグレード後にアプライアンスを再起動する必要があります。

このリリースでサポートされているハードウェア

- すべての仮想アプライアンスモデル
- 次のハードウェア モデル
  - C380、C390、C680、または C690
  - C190

    アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『*Cisco コンテンツ セキュリティ仮想アプライアンス インストール ガイド*』を参照してください。このドキュメントは https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースが 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンスを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシンインスタンスを導入する必要があります。

仮想アプライアンスをアップグレードしても、既存のライセンスは変更されません。

ハードウェアアプライアンスから仮想アプライアンスへの移行

ステップ 1 仮想アプライアンスの展開またはアップグレード（13 ページ）で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェアアプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされたハードウェアアプライアンスから設定ファイルを保存します。

ステップ 4 ハードウェアアプライアンスから仮想アプライアンスに設定ファイルをロードします。

ネットワーク設定に関連する適切なオプションを選択してください。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『*Cisco コンテンツ セキュリティ仮想アプライアンス インストール ガイド*』に記載されています。

以下のサービスとサポート（21 ページ）も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

- RSA DLP Suite および RSA Enterprise Manager はサポート対象外（15 ページ）
- C100V モデルのパフォーマンスの低下（15 ページ）
- FIPS の準拠性（15 ページ）
- AsyncOS の以前のバージョンへの復元（15 ページ）
- 集中管理（クラスタ化されたアプライアンス）を使用した展開のアップグレード（15 ページ）
- 直前のリリース以外のリリースからのアップグレード（16 ページ）
- 設定ファイル（16 ページ）
- アップグレード中の IPMI メッセージ（16 ページ）

RSA DLP Suite および RSA Enterprise Manager はサポート対象外

RSA は、RSA Data Loss Prevention Suite（DLP）のサポート終了（EOL）を発表しました。シスコは、RSA DLP で作成されたすべての既存の DLP ポリシーを新しい DLP エンジンへとシームレスに移行できる、代替の DLP ソリューションを提供します。アップグレード後は、Web インターフェイスの [Security Services] > [Data Loss Prevention] ページで、移行した DLP ポリシーを表示または変更できます。詳細については、ユーザ ガイドの「Data Loss Prevention」の章を参照してください。

Async0S 11.0 以降は、RSA Enterprise Manager の統合のサポートはありません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。

C100V モデルのパフォーマンスの低下

C100V モデルで AsyncOS 11.1 にアップグレードすると、特定の設定でパフォーマンスが低下する可能性があります。詳細については、以下を参照してください。

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCve27500

FIPS の準拠性

AsyncOS 11.1 リリースは、FIPS 準拠のリリースではありません。アプライアンスで FIPS モードを有効にしている場合は AsyncOS 11.1 にアップグレードする前に FIPS モードを無効にする必要があります。

AsyncOS の以前のバージョンへの復元

次の AsyncOS バージョンは、内部テスト インターフェイスの脆弱性（http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa）の影響を受けます。

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

集中管理（クラスタ化されたアプライアンス）を使用した展開のアップグレード

クラスタに C160、C360、C660、X1060、C170、C370、C670、または X1070 ハードウェア アプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x60 および x70 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x60 および x70 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー(AsyncOS X.0)またはマイナー(AsyncOS X.x)リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース(AsyncOS X.x.x)には、バグ修正のみが含まれています。

設定ファイル

通常、シスコは、以前のメジャーリリースに関して、設定ファイルの下位互換性をサポートしていません。マイナーリリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコカスタマーサポートでご確認ください。

アップグレード中の IPMI メッセージ

CLI を使用してアプライアンスをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。これは既知の問題です。

障害 ID:CSCuz28415

メッセージの DMARC 検証中のエラー

このリリースにアップグレードして DMARC を有効にすると、DMARC ドメイン名を含むが、DNS 内の一致するテキスト レコードは含まない DMARC レコードをアプライアンスが取得するときに、DNS の永続的なエラーが発生する場合があります。これは既知の問題です。

障害 ID:CSCvp82960

このリリースへのアップグレード

はじめる前に

- 既知および修正済みの問題(18 ページ)とインストールおよびアップグレードに関する注意事項(13 ページ)を確認してください。
- 仮想アプライアンスをアップグレードする場合は、仮想アプライアンスのアップグレード(14 ページ)を参照してください。

手順

Email Security Appliance をアップグレードするには、次の手順を実行します。

ステップ 1 アプライアンスから、XML 設定ファイルを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合は、アプライアンスからセーフリスト/ブロックリストデータベースをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。

ステップ 4 キューが空になるまで待ちます。

ステップ 5 [システム管理(System Administration)] タブで、[システムアップグレード(System Upgrade)] ページを選択します。

ステップ 6 [利用可能なアップグレード(Available Upgrades)] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。

ステップ 7 [アップグレードの開始(Begin Upgrade)] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。

ステップ 8 アップグレードが完了したら、[今すぐリブート(Reboot Now)] ボタンをクリックしてアプライアンスを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[システム管理(System Administration)] > [SSL 構成(SSL Configuration)] ページを使用するか、CLI で `uuneqphki` コマンドを使用します。手順については、ユーザガイドまたはオンラインヘルプの「System Administration」の章を参照してください。
- 「パフォーマンスアドバイザリ (18 ページ)」を確認してください。

アップグレード後の注意事項

AsyncOS 11.x へのアップグレード後のクラスタ レベルでの DLP 設定の不整合

AsyncOS 11.x にアップグレードした後、アプライアンスがクラスタ モードになっていて、DLP が設定されている場合、CLI を使用して `clustercheck` コマンドを実行すると、DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次の例に示すように、`clustercheck` コマンドで「`How do you want to resolve this inconsistency?`」というプロンプトを使用します。

```
*(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

パフォーマンスアドバイザリ

DLP

- 着信メッセージに対してスパム対策およびウイルス対策スキャンがすでに実行されているアプライアンスで発信メッセージの DLP を有効にすると、10 % 未満のパフォーマンス低下が発生する可能性があります。
- 発信メッセージだけを実行し、スパム対策およびウイルス対策が実行されていないアプライアンスで DLP を有効にすると、前のシナリオと比べてパフォーマンスがさらに低下する可能性があります。

SBNP

SenderBase Network Participation では、コンテキスト適応スキャン エンジン（CASE）を使用してデータを収集し、IronPort 情報サービスを駆動するようになりました。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズまたは X シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されているアプライアンスの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20 % 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツ セキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

- バグ検索ツールの要件（18 ページ）
- 既知および修正済みの問題のリスト（19 ページ）
- 関連資料（20 ページ）

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

AsyncOS 11.1.3 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.3&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.3-009&sb=fr&bt=custV

AsyncOS 11.1.2 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.2*&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.2-023&sb=fr&bt=custV

AsyncOS 11.1.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.1&sb=afr&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.1-042&sb=fr&bt=custV

AsyncOS 11.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.0&sb=afr&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.1.0&sb=fr&bt=custV

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [E メールセキュリティ(Email Security)] > [Cisco E メールセキュリティアプライアンス(Cisco Email Security Appliance)] の順にクリックし、[OK] をクリックします。

ステップ 4 [リリース(Release)] フィールドに、リリースのバージョン(たとえば、11.1.3)を入力します

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから、[これらのリリースで修正済み(Fixed in these Releases)] を選択します。
- 既知の問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから [これらのリリースに影響(Affecting these Releases)] を選択し、[ステータス(Status)] ドロップダウンから [開く(Open)] を選択します。

(注) ご不明な点がある場合は、ツールの右上にある [ヘルプ(Help)] または [フィードバック(Feedback)] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索(search)] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

マニュアルの内容 (Cisco Content Security 製品)	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco コンテンツ セキュリティ管理	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco E メール セキュリティ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html

マニュアルの内容 （Cisco Content Security 製品）	参照先
Cisco コンテンツ セキュリティ アプライアンスの CLI リファレンス ガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマー サポートにアクセスすることもできます。手順については、ユーザ ガイドまたはオンライン ヘルプを参照してください。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。