VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Vanguard Integrity Professionals

BM z/OS® セキュリティー・サーバー向け
セキュリティーならびにコンプライアンス・ソフトウェア製品
バージョン 2.3

新機能概要

2017 年 10 月 06 日

エグゼクティブ・サマリー

Vanguard Integrity Professionals は、IBM z/OS セキュリティー・サーバー向けのバージョン 2.3 のセキュリティーならびにコンプライアンス・ソフトウェア製品の発売と即時使用可能を発表しました。このバージョンの Vanguard ソフトウェアは、旧バージョンのほぼすべての面で向上し、データの機密保護が極めて重要である場合は、広範囲の新しい特性と機能を提供します。

Vanguard の最新バージョン 2.3 のソフトウェア製品には、100 個を超える新しい特性と機能拡張が含まれており、お客様がより高いレベルのセキュリティー、より高度な制御および、あらゆるサイバー・セキュリティーの課題に、今までになく迅速に対応できるようになります。

- Vanguard Enforcer は、新しいアクセサ環境要素 (ACEE) センサーを含みます。そのセンサーは、セキュリティー・サーバーの定義とは異なる ACEEs に含まれ高くされた権限を検出しレポートします。
- 多要素認証で、セッション管理とエンタープライズ認証がサポートされるようになりました。
- Vanguard Policy Manager は、新しいコマンド・ポリシーを含みます。それはユーザーまたはグループに接続されたユーザーへの変更を防ぎます。
- Policy Manager は、RACF データベース内の特定のプロファイルまたはすべてのプロファイルへの変更をレポートする新しい機能を供給します。
- RSA SecurID 用の Vanguard ez/Token は、多要素認証のために RACF パスワード、RSA PIN およびトークンの使用をサポートするようになりました。
- すべての Vanguards Active Alerts との SIEM 統合。
- Vanguard ez/Token は、PING、DUO、LinOTP および他のバックエンド認証サーバーをサポートするようになりました。
- サポートされるプラットフォーム間でパスワードを同期する機能。
- まったく新しい Vanguard HelpDesk ソリューション。
- ベスト・プラクティスは、Vanguard Configuration Manager に含まれるようになりました。

デジタル変換は定着し、企業により生成されるデータとトランザクション量が増加し、アプリケーションの変更率が高まりました。その結果、計算、ストレージおよびネットワーク資源のより良い利用につながる、より柔軟で拡張性のあるソフトウェア駆動型のインフラストラクチャーが必要となります。

IBM の z/OS V2.3 オペレーティング・システムと、Vanguard Integrity Professionals のサイバー・セキュリティー・ソフトウェア V2.3 は、高度な拡張性と安全性に優れた次世代インフラストラクチャーを構築するためのイノベーションを提供します。Vanguard V2.3 は、デジタル変換の要求を満たすために必要なパフォーマンス、可用性、そしてセキュリティーを提供します。

今日のメインフレームは、世界的な商取引の中心で、世界の最も要求の厳しい取引要件を担当しています。そして次のことを支えています：

- すべてのクレジット・カード取引の **87 パーセント**、年間約 **8 兆ドル**の支払い。
- 毎年 **290 億件**の ATM 取引、1 日あたり約 **50 億ドル**相当の価値。
- 毎年 **40 億人**の航空便。
- 1日あたり **300 億件**以上の取引 – 毎日の Google 検索数を上回る。
- IT コストの総額の 6 パーセントのみで、世界の生産仕事量の **68 パーセント**。

金融サービス業界の銀行などは、世界の金融システム活動を保つめに、毎秒数千件の取引を処理します。メインフレームは、大量の取引データを確実に取り扱うために、これまで以上に重要性が増しています。

世界の上位 100 位に入る銀行の 92 社は、膨大な量の取引を効率的に処理できるメインフレームの能力のために、メインフレームに依存しています。クラウド時代に金融サービス機関が効率的に競争できるように、取引により生成された膨大な量の機密データを、IBM Z を使用して日々の業務を中断させることなく、不正行為やサイバー犯罪から保護し、分析し収益化することができます。

サマリー
今日の経済環境では、膨大な情報を迅速に消費、操作、配信し、クラウド・サービスの機能を利用してビジネスにおける洞察を抽出する必要があります。その情報は、安全に管理され、処理され、世界中に配信されなければなりません。伝統的な処理からのこのような基本的な転換は、データ・セキュリティーの最適水準を維持しながら、極めて重要な作業のサービス・レベルに影響を与えることなく、新しい作業負荷をサポートできる高い応答性と信頼性のあるプラットフォームを必要としています。

以下のリストは、IBM z/OS セキュリティー ・サーバー用の Vanguard Integrity Professionals のセキュリティーならびにコンプライアンス・ソフトウェア製品のバージョン 2 リリース 3 の主要機能の概要を示しています。

Vanguard Active Alerts™

警告通知での多要素認証のサポート

説明

警告通知処理に多要素認証のサポートが追加されました。ALTUSER、 RALTER および RDEFINE コマンドが生成される時に、新しい多要素認証のパラメーターが組み込まれます。

利点

コマンドが生成される時に、新しいコマンド・パラメーター、サブ・パラメーターおよびそれらの値が完全なコマンドに追加され、正確に表示されます。

コマンド生成における RACF コマンド・パラメーターとサブ・パラメーターのサポート

説明

新しい z/OS セキュリティー・サーバー (RACF) V2R3 のコマンド・パラメーターとサブ・パラメーターを含めるためのサポートが追加されました。

利点

コマンドが生成される時に、新しいコマンド・パラメーター、サブ・パラメーターおよびそれらの値が完全なコマンドに追加され、正確に表示されます。

Vanguard Active Alerts における SIEM のサポートの追加

説明

Vanguard Active Alerts にセキュリティー情報およびイベント管理 (SIEM) のサポートを追加。

利点

お客様は、z/OS メインフレームのセキュリティー・イベント情報を集中型の SIEM ソリューションへ送信できます。そしてその SIEM ソリューションはイベントのレポート処理と相関を可能にします。このことは、メインフレーム用の個別のソフトウェアを必要とせずに、時間、資金および労力を節約し、お客様が監査要求事項を達成することを支援します。

SIEMMSGFORMAT 値のサポートの追加

説明

CEF メッセージの先頭に Syslogd RFC ヘッダーが付くことを示すために、SIEMMSGFORMAT に 11 という数値のサポートが追加されました。この値は、対象の SIEM ARCSIGHTUDP および ARCSIGHTTCP に対してのみサポートされます。

利点

イベント・データを ARCSIGHTUDP または ARCSIGHTTCP へ送信する際の柔軟性をユーザーに提供します。

追加の DB2 イベントを組み込むために Alert 16 を強化

説明

クラス 4 と 5 がトレースされている場合、First Read (IFCID 143)と First Write (IFCID 144)を含めるように、Alert 16 にサポートが追加されました。

利点

PCI または PII データが DB2 テーブルに収容されている場合、監査員の関心があり、自動化に利用できる、システム上の追加の DB2 活動を警告することができます。

パスワードおよびパスワード・フレーズの変更をカウントし追跡するために Active Alert 7 を強化

説明

RACF パスワードとパスワード・フレーズの変更をカウントし追跡する機能が追加されました。

利点

パスワードとパスワード・フレーズの変更に警告する機能。不審な活動が疑われる時に、監査員は、この機能拡張に関心を持ち、この機能を使用して自動化することができます。

通知として送信するイベントの範囲を制限

説明

Vanguard Active Alerts (VAA)およびセキュリティー情報およびイベント管理 (SIEM)のマスキング・パラメーター LEVEL のサポートが追加されました。このパラメーターは Alerts VIO、AA5 および AA13 でサポートされます。

VAA および SIEM のマスキング・パラメーターTABOWNER のサポートが追加されました。このパラメーターは Alert AA16に関してサポートされます。

利点

この機能拡張により、管理者および監査員は、追加のマスキング機能により、警告通知として送信されるイベントの範囲を絞り込むことができます。管理者と監査員は、関心のある特定のイベントに焦点を絞ることができるようになりました。

SIEM 処理のためのイベント・データの配布を調整する能力

説明

ユーザーは次のことができます：

それぞれの警告にデフォルトの Syslogd 重要度を割り当てます。
その Syslogd 重要度を、VAAOPTxx メンバー内の新しいパラメーターを使用して、または通知タスクへの MODIFY コマンドを使用して、変更します。

利点

追加のオプションにより、セキュリティー情報およびイベント管理 (SIEM) 処理のためのイベント・データの配布を調整できます。これにより管理者と監査員が追加の特定の情報を取得するのに役立ちます。その特定の情報は、関心のある特定のイベントに焦点を絞るのに役立ちます、そして優先度の高いイベントを調査の最上位に送ることができます。

MODIFY STATS および MODIFY DIAG コマンド出力の向上

説明

データ・コレクターMODIFY STATS および MODIFY DIAG コマンドの出力表示が拡張されました。捕獲される SMF レコード・タイプそして各警告で使用される SMF レコード・タイプを文書化するために *Vanguard Active Alerts Installation and Administrator Guide* が更新されまました。

利点

拡張された表示には、Vanguard Active Alerts とセキュリティー情報およびイベント管理 (SIEM) の設定および通知として処理され送信されたイベント数の追加の情報が含まれます。この機能拡張は、管理者と監査員が問題の診断と実装の有効性の追跡の両方を行うにみ役立ちます。

ROAUDIT 属性のサポート

説明

ALU, AU コマンドの ROAUDIT 属性のサポートが追加されました。

利点

ROAUDIT が、新しいユーザーに割り振られるまたは取り去られる、または既存のユーザーに割り振られるまたは取り除かれる時に、警告が監査員へ送信され、監査員は特権が適切に割り振られたことを確認するためにその警告を使用できます。また、過去の追跡目的のために、セキュリティー情報およびイベント管理 (SIEM) に警告を送信することができます。

通知タスクの性能の向上

説明

通知タスクは、VAARTNxx オプション・メンバー内のユーザー選択基準を処理する時の VIPOPTS データセットへの I/O を削減するように拡張されました。
通知タスクは、VAARTNxx メンバー内の更新されたユーザー選択基準を、通知タスクを再起動しなくても、MODIFY コマンド経由で使用できるように拡張されました。
Enforcer オプション・メンバーとパラメーター(VANSAMP メンバーVAACVEA) および Advisor オプション・メンバーとパラメーター (VANSAMP メンバーVAACVSR) に変換するユーティリティーは、コメントとしてあらゆる新しい VAAOPTxx パラメーターを含めるように更新されました。

利点

性能の向上とシステム資源の使用量の削減。

MODIFY STATS 表示の向上

説明

Vanguard Active Alerts Installation and Administrator Guide 内で簡単に説明できるように、MODIFY STATS 表示内に警告イベント数が含められ、統計メッセージにメッセージ番号を割り当てられました。

利点

一元的の代わりに個別に文書化することにより、それぞれの統計表示の理解が容易になります。

Vanguard Administrator™

Vanguard Password Administration の紹介

説明

Vanguard は Vanguard Identity Manager (VIM) のすべての機能を取り入れ、そのウェブ版を開発しました。

利点

お客様は、VIM のすべての機能性を備えた使いやすいウェブサイトに立ち寄り、そしてメインフレームまたは分散プラットフォーム上でそれを自然にホストすることができるようになりました。

Vanguard Password Administration により、ヘルプ・デスクや他の管理者は、ドロップインからすべての VIM 機能を実施、簡単に使用、そしてウェブサイトを管理できます。この新しい機能により、単一のウェブサイトから VIM の目的ですべてのシステムを管理できます。

これにより、グリーン・スクリーン技術や RACF に詳しくない新規ユーザーは、IBM メインフレーム・プラットフォームのトレーニングや深い知識がなくても、すべての VIM 機能を実施できます。

この新しいウェブサイトは使いやすく、中央または分散管理者が VIM 活動を実施できるようにし、システム全体でこれを可能にします。

IBM z/OS 2.3 許容範囲サポート

説明

この Vanguard Administrator への機能拡張により、IBM z/OS バージョン 2.3 に対する許容範囲サポートが追加されました。

利点

Vanguard 製品は、IBM z/OS リリースで最新の状態を支持するために継続的に更新されています。この許容範囲サポートは Vanguard Administration 製品のバージョン 2.2 および 2.1 にも追加されました。

ユーザーWORKATTR 電子メール・アドレスのサポート

説明

ユーザー・レポート・オプションは、RACF 2.3 以降の新しいユーザーWORKATTR セグメントの電子メール・アドレス・フィールドをサポートするために更新されました。更に、クローンとリビルドのユーザー・コマンド処理はこの新しいフィールドをサポートするために更新されました。この機能拡張は、Vanguard Administrator のオンラインおよびバッチ処理に適用されます。

利点

RACF 2.3 サポート。

VIPOPTS DD ステートメントにリストされている複数のライブラリーのサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して複数のライブラリーを指定する機能が追加されました。活動中のオンライン・セッションに割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに複数のライブラリーを指定する機能が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み込みます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

この機能により、複数のシステムが VIPOPTS DD ステートメント定義を共有することが可能になり、各システム用の各 VIPOPTS ライブラリーでこの情報を複製する必要はありません。

SHOWNOTE トグル機能を追加

説明

「SHOWNOTE」トグル機能が、データセットおよび一般リソース・パネルに追加され、最上部にある各レポート・オプションに特有のマスキングとその他の注記が表示されなくなります。その注記が抑止される場合、実際のマスキング・フィールドの多くがパネルに表示されます。

利点

この機能拡張により、スクロールしなくても、初期のレポート・パネルに表示されるマスキング・フィールドを多く表示することができます。

ROAUDIT および NOROAUDIT オペランドのサポート

説明

Vanguard Administrator のこの機能拡張により、IBM z/OS バージョン 2.2 用の開発サポートが作成されました。

利点

Vanguard 製品は、IBM z/OS リリースで最新の状態を支持するために継続的に更新されています。この開発サポートにより、Vanguard Administrator のコマンド生成と VRC に、ROAUDIT と NOROAUDIT が追加されました。

RACF の新しいパスワード暗号化アルゴリズム (KDFAES) のサポート

説明

Vanguard Administrator のこの機能拡張により、IBM APAR OA43999 の開発サポートが作成されました。

利点

Vanguard 製品は、IBM z/OS リリースおよび APARS で最新の状態を支持するために継続的に更新されています。この開発サポートにより、Vanguard Administrator のコマンド生成と VRC に、新しいパスワード・アルゴリズム KDFAES のサポートが追加されました。

ユーザーID に接続されたグループ名をマスクする機能

説明

ユーザー・レポートのユーザーID に接続されたグループ名をマスクする機能を追加しました。

利点

Vanguard 製品は、お客様の要件と情報に基づいて継続的に更新されます。セキュリティー管理者は、どのユーザーが特定のグループに接続しているかを調査することが、簡単にできるようになりました。

ALTUSER コマンドで EXPIRED オペランドのサポート

説明

ユーザー・パスワードに EXPIRED オペランドを指定する機能が追加されました。

利点

Vanguard 製品は、IBM z/OS の変更を基に継続的に更新されます。z/OS の IBM APAR OA43999 は、ユーザーに彼らのパスワードを失効させる機能を導入しました。この機能拡張により、Vanguard Administrator 製品は ALTUSER コマンドの EXPIRED オペランドをサポートすることができます。

VRC で EXPIRED オペランドのサポート

説明

Vanguard Administrator の VRC 機能で、ユーザーの EXPIRED オペランドを指定する機能が追加されました。

利点

Vanguard 製品は、IBM z/OS の変更に基づいて継続的に更新されます。z/OS の IBM APAR OA43999 は、ユーザーに自身のパスワードを失効させる機能を導入しました。この機能拡張により、VRC は、VRC コマンドで指定されたユーザーの ALTUSER コマンドに EXPIRED オペランドを設定し生成することができます。

変更された PASSWORD オペランドのサポート

説明

CLONE、REBUILD およびユーザーID を作成している間に、PASSWORD オペランドが指定される方法を変更します。

利点

Vanguard 製品は、IBM z/OS の変更に基づいて継続的に更新されます。z/OS の IBM APAR OA43999 は、PASSWORD または PHRASE オペランドが PW と AU コマンドに指定されていない場合、（パスワードを既知の値へセットするのではなく）新規ユーザーが保護されているという要件が導入されました。この機能拡張により、保護されたユーザーを作成することを回避するために AU コマンドに PASSWORD オペランドが生成され指定されているようなユーザーを、Vanguard Administrator が作成する方法を変更します。

SVSAM および MVSAM ファイル名の検証

説明

エクストラクト指定の重複データセット名検査。

利点

お客様は定期的に、Vanguard Administrator への入力データとして、SVSAM と MVSAM エクストラクト・ファイルのファイル名の指定を間違えます。Vanguard Administrator は、名前を検証することなしに、いつもお客様の入力データを受け取りそして処理していました。

この機能拡張により、Vanguard Administrator は、レポートの実行やコマンドの生成を試みる前に、基本的な入力データ検証を実施するようになりました。この機能拡張により、お客様が処理のために必要な SVSAM と MVSAM ファイルの指定の準備を支援します。

レポート処理性能の向上

説明

データセットおよび一般リソース・レポートの性能が向上しました。

利点

データセットおよび一般リソース・レポートは、ライブとエクストラクト・モード (オンラインとバッチ) の両方のレポート処理に性能の向上を追加することにより、アップグレードされました。

コマンド生成における EXPIRED パスワードのサポート

説明

ユーザー・パスワードに EXPIRED オペランドを指定する機能が追加されました。

利点

Vanguard 製品は、IBM z/OS の変更に基づいて継続的に更新されます。z/OS の IBM APAR OA43999 は、ユーザーが自身のパスワードを失効させる機能を導入しました。この機能拡張により、お客様は、コマンド生成時にユーザーのパスワードが失効するように設定するだけでなく、データベースの中を探しすべてのユーザー (TSO、DB2、CICS および他の区分のユーザー) を見つけることができます。ユーザーを簡単に失効できるようになります。データベース内のすべてのユーザーは、単一のコマンド生成処置によって、失効させることができます。

RACF コマンド PWCONVERT と PWCLEAN のサポート

説明

ユーザーID に PWCONVERT と PWCLEAN を指定する機能が追加されました。

利点

Vanguard 製品は、IBM z/OS の変更に基づいて継続的に更新されます。z/OS の IBM APAR OA43999 は、ユーザーが自身のパスワードを AES へ変換し、パスワード履歴をクリーン/クリアーする機能を導入しました。この機能拡張により、お客様は、Vanguard Administrator の VRC インターフェイスを通して、PWCONVERT と PWCLEAN オペランドを指定することができます。

Vanguard Advisor™

VIPOPTS DD ステートメントにリストされている複数のライブラリーをサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して複数のライブラリーを指定する機能が追加されました。活動中のオンライン・セッションに割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに複数のライブラリーを指定する機能が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み込みます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

この機能により、複数のシステムが VIPOPTS DD ステートメント定義を共有することが可能になり、各システム用の各 VIPOPTS ライブラリーでこの情報を複製する必要はありません。

新しいレポート: ファイル・システム活動

説明

SMF 92 レコードを使用した、ファイル・システム活動サマリーおよび詳細標準レポートのサポートが追加されました。

利点

システム上のファイル・システム活動に対する認識を高めます。

新しいレポート: TCP/IP 標準サマリーと詳細レポート

説明

機能拡張により、「TCP Server Connection Termination」および「TCP Client Connection Termination」という名前の新しい TCP/IP 標準サマリーおよび詳細レポートが追加されました。これらのレポートは、オンラインおよびバッチ・レポートとしてサポートされ、SMF 119 サブタイプ 2 レコードを使用します。

利点:

このレポートは、システム上の TCP/IP 活動に対する認識を高めます。

新しいバッチ・レポートのオプション: NOSORT

説明

バッチ・レポートに NOSORT パラメーターのサポートが追加されました。そのパラメーターは、レポート・データがソートされるものではないことを示します。

利点:

見出しなしにデータ・ファイルを作成し、フラット・ファイルにそれを収納するために、必要に応じてレポート処理を高速化することができます。ユーザーは、データをソートする必要のないアプリケーションへデータを送信することも、ソートされていないデータを QuickGen で処理して、セキュリティー情報およびイベント管理 (SIEM)ソリューションなどのアプリケーションへ送信することもできます。

新しい MLS およびセキュリティー・イベント・レポート

説明

機能拡張により、MLS およびセキュリティー・イベント標準レポートに対する SMF レコード・タイプ 83 サブタイプ 3 (LDAP 監査データ) のサポートが追加されました。

利点

このレポートは、システム上のセキュリティー関連活動に対する認識を高めます。

多要素認証サポートを追加

説明

Advisor のレポート作成処理に、多要素認証 (MFA) のサポートが追加されました。

1. ALTUSER、RALTER および RDEFINE コマンドが生成された時に、新しい MFA パラメーターが組み込まれます。
2. サインオン・イベントを含むレポートに、新しいイベント修飾子コード 40-42 のイベントを含めるようになりました。

利点

1. コマンド生成処理は、すべてのパラメーター、サブ・パラメーターおよびそれらの値をレポート作成用に正確に表示します。
2. サインオン・イベントは、MFA 処理により生成されます。

DB2 レポートを強化

説明

機能拡張により、監査対象テーブル・サマリーおよび詳細レポートに対する DB2 活動に、SMF 102 IFCIDs 143 (監査対象オブジェクトへの最初の書き出し) および 144 (監査対象オブジェクトへの最初の読み込み) が追加されました。

利点

システム上の DB2 活動の詳細情報を提供します。

生成されるコマンドに新しいコマンド・パラメーター、サブ・パラメーターの組み入れ

説明

新しい z/OS セキュリティー・サーバー (RACF) V2R2 のコマンド・パラメーターおよびサブ・パラメーターを組み入れるためのサポートが追加されました。

利点

生成されたコマンドに、新しいコマンド・パラメーター、サブ・パラメーターおよびそれらの値が含まれるようになり、正確に表示されます。

zEDC 圧縮ログ・ストリームのサポート

説明

zEDC 圧縮 SMF ログ・ストリームのサポートが追加されました。

利点

圧縮されたログ・ストリームを活用し、Advisor のレポート機能を維持できます。

JCL 生成の強化

説明

Advisor JCL 生成処理に、連結される VIPOPTS データセット名を組み入れるサポートが追加されました。それらのデータセット名は、VANLIBS または VSROPT00 オプション・メンバーに

VIPOPTS パラメーターを使用して指定されます。または VIPOPTS パラメーターが指定されていない場合には、ログオン割り振りの VIPOPTS DD ステートメントから指定されます。

利点

オプション・パラメーターは、別のライブラリーに配置することにより、共有できます。すべてのユーザーに影響を与えずにオプション・パラメーターをカストマイズできます。

エクストラクトの自動構築

説明

Advisor エクストラクトを構築する JCL の自動構築が追加されました。活動中の MAN データセットと指定された過去日数のダンプ・データセットから構築します。

利点

この機能拡張により、ユーザーは現在から N 日前のエクストラクトを作成するための JCL を生成できます。エクストラクトの作成処理は、命名規則を基に必要な JCL を自動的に構築し、すべての MAN ファイルとエクストラクト・ファイルが取得されます。それは、レポート目的で使用できる単一のエクストラクト・ファイルを作成するためです。これにより、ファイルの手作業による介入と指定が削減または排除されます。それは活動中の SMF データと何日も過去のエクストラクトの両方を使用してレポートを集約する場合です。

Vanguard Analyzer™

VIPOPTS DD ステートメントにリストされている複数のライブラリーをサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して複数のライブラリーを指定する機能が追加されました。活動中のオンライン・セッションに割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに複数のライブラリーを指定する機能が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み込みます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

この機能により、複数のシステムが VIPOPTS DD ステートメント定義を共有することが可能になり、各システム用の各 VIPOPTS ライブラリーでこの情報を複製する必要はありません。

新しいレポート: Unix アイデンティティー分析

説明

この新しいレポートは Analyzer に追加され、UNIX ユーザーとグループ・アイデンティティーの自動割り当てに必要な RACF プロファイル情報が表示されます。

利点

すべての Unix RACF 関連情報は、単一のスクリーンおよびバッチ・レポートに統合されます。AIM ステージ・レベルと同様に、理想的な AIM レベルに達するための追加情報と推奨の支援も提供されます。

機密で重要なデータセット分析でシステム記号をサポート

説明

機密で重要なデータセット分析 (バッチおよびオンライン) に追加されたサポートにより、ユーザー定義のデータセット・リスト内に、またはデフォルトの Vanguard VIPLST データセットを 置き換えるための VIPLST データセット・リストを定義した時に、ユーザーはシステム記号を使用できます。

利点

この機能拡張により、ユーザーは、システム間で唯一の違いが記号の値である場合に、システム間で共用できるファイル内にデータセット名を指定することができます。

VIPLST および USERDSN のデータセット名でシステム記号をサポート

説明

データセット名に、SMFID を取得するための SYSSMFID に加えて、Vanguard Analyzer が実行しているシステム上で定義されたあらゆる記号を含めることができます。

利点

この機能拡張により、ハードコードされた値ではなく、記号パラメーターを使用することができます。

機密で重要なデータセット分析の LNKAUTH メッセージ

説明

LNKAUTH 指定と LNKAUTH ステートメントが見つかった IEASYSxx メンバーを示す一般メッセージが追加されました。

利点

重要な APF データセットの RACF 情報は、オンラインとバッチですぐに利用可能です。

データベース分析レポートで AIM ステージ・レベルを表示

説明

アプリケーション・アイデンティティー・マッピング (AIM) ステージ・レベルが、データベース分析オンラインおよびバッチ・レポートに表示されるようになりました。

利点

Unix RACF AIM ステージ情報は、データベース分析レポートの一部としてすぐに利用可能です。

Vanguard Cleanup™

VIPOPTS DD ステートメントにリストされている複数のライブラリーをサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して複数のライブラリーを指定する機能が追加されました。活動中のオンライン・セッションに割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに複数のライブラリーを指定する機能が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み込みます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

この機能により、複数のシステムが VIPOPTS DD ステートメント定義を共有することが可能になり、各システム用の各 VIPOPTS ライブラリーでこの情報を複製する必要はありません。

VRA エクストラクト・ファイルと Vanguard Offline 製品の互換性検査を追加

説明

1. VRA エクストラクト・ファイルと Vanguard Offline 製品の互換性検査が追加されました。
2. 内部 I/O パフォーマンスとメッセージ生成の改善。

利点

この互換性検査により、Vanguard Offline 製品が VRA エクストラクト・ファイルのデータを最大限に活用することを確認することで、 正確なレポートを得ることができます。

レポートの入力として複数の履歴マスター・ファイルの指定

説明

ユーザーが、レポートの入力として複数の履歴マスター・ファイル (HMF) を指定できるようになりました。

利点

この機能拡張により、Vanguard Offline 製品は複数の HMF をレポートの入力として使用できます。複数の HMF の使用により、複数の LPAR にわたってレポートすることができます。それは一回の実行で、あらゆるレポートについて、一つの RACF データベースまたは様々なデータベースに対して実施できます。レポートとコマンド検査が複数システム間で可能になりました。

新しいマスキング・フィルターはキャプチャー・フィルタリング時により高い精度を追加

します

説明

フィルタリングされるリソースの精度を提供する新しい VCL および VOF フィルターが追加されました。

利点

新しいマスキング・フィルターが追加され、キャプチャー・フィルタリング中により詳しく細かい指定が可能になりました。

この機能拡張により、お客様は収集のために望ましくないデータのフィルタリングを指定することができます。そのデータは通常 Vanguard Offline および Vanguard Cleanup により収集される膨大な量のデータです。

履歴収集のクリーンナップとアクセス・レポートの検証

説明

履歴収集をクリーンナップし、アクセス・レポートを検証するたに強化されたマスキングが追加されました。

利点

クリーンナップ履歴詳細および検証 (x) レポートが強化され、利用可能な特定のレポートのマスキングが強化されました。

お客様は、レポートされるデータに対して、より特定のレポートを、より迅速により詳細に取得できます。

Vanguard Configuration Manager™

VCM における DoD DISA STIG の最新バージョンへの対応

説明

最新セキュリティー・テクニカル実装ガイド (STIG)サポートが追加されました。Vanguard Configuration Manager (VCM)は、アメリカ国防総省 (DoD) の国防情報システム局 (DISA) からの最新の検査で、3 か月ごとに更新されます。

利点

VCM を所有することの大きな利点は、VCM は DoD DISA STIG の最新バージョンに常に更新され維持されることです。つまり、3 か月ごとに新しい検査基準が作成され、お客様に利用可能になります。

Vanguard Configuration Manager (VCM) は、DoD DISA STIG の最新かつ最も厳格なコンプライアンス製品です。お客様がどんな変更が成されたかを識別するまたは追跡する必要がなく、常に DISA STIG の変更の最新バージョンを所有できるように、継続的に VCM を維持します。VCM は

継続的に更新され、そしてそのインターフェイスはお客様に新しい検査と修正された検査を通知します。

Vanguard Best Practices は、Vanguard Configuration Manager に組み込まれました

説明

Vanguard は、新しい検査を、Vanguard Configuration Manager の Vanguard Best Practices という名前の新しいセクションに追加しました。Vanguard Best Practice 検査は、お客様の現在のセキュリティー設定と IBM z/OS の構成設定を、Vanguard Integrity Professionals が推奨し Vanguard Best Practices に体系化されている設定と比較します。

利点

Vanguard Best Practices は、Vanguard Configuration Manager に組み込まれました。Vanguard プロフェッショナル・サービスの支援により、VCM のお客様は、お客様の現在のセキュリティー設定と Vanguard Integrity Professionals の推奨する設定を比較できるようになりました。

新しい検査: 実行計画とマイルストーン

説明

実行計画とマイルストーン。

利点

Vanguard Configuration Manager (VCM) により、検査により報告された調査結果を改善するために、お客様の現在の実行計画とマイルストーンを検査することができるようになりました。レポートが実行される時に、選択され参加する場合、実行計画とマイルストーンの情報は、レポートに含まれるだけでなく、VCM インターフェイスを経由して表示および更新可能になります。

この機能拡張により、お客様はすべての関連情報と実行を保つことができます。その実行は、一か所の VCM により追跡される調査結果を解決するために行われます。

VCM レポートの新しいオプション: SKIPNORECS

説明

オプション SKIPNORECS が追加されました。

利点

このオプションをレポート処理に指定した場合、Vanguard Configuration Manager (VCM) は検出されなかった検査のレポートをスキップします。

VCM に基づいた調査結果のレポート改善に取り組む時に、お客様は通常レポートの調査結果のみを検査します。この新機能により、レポート中に調査結果が得られない検査のレポートを容易に入手できます。そしてこれには決して実行されかった検査が含まれます。

QuickGen が VCM に追加されました

説明

Vanguard QuickGen 機能が Vanguard Configuration Manager (VCM) に追加されました。

利点

VCM で、お客様が Vanguard QuickGen を使用して独自のレポートを作成できるようになりました。Vanguard QuickGen を使用すると、データを手作業でエクスポートおよび操作することなく、監査員、管理者などが要求する特別レポートを作成できます。

ユーザーによる特別レポートを提供します。さらに、SMFID および SYSID がレポート用に利用可能なフィールドとして追加されました。

VCM レポートの日付形式をカストマイズする機能

説明

日付形式のサポート。

利点

Vanguard Configuration Manager (VCM) は、お客様が VCM レポートの日付の特定の形式を指定できるように拡張されました。

検査結果インターフェイスから FIND コマンドを発行

説明

FIND コマンドを、検査結果インターフェイスから発行できるようになりました。

利点

Vanguard Configuration Manager (VCM) の検査結果インターフェイスが変更され、検査結果セット内で FIND コマンドを発行できるようになりました。以前は、特定のデータを見つけるためにレポートを実行する必要がありました。このサポートの一部として、X ALL と他の ISPF コマンドも、新しいインターフェイスで使いやすさのために使用できます。

Vanguard Configuration Manager に自動データ収集を追加

説明

Vanguard Configuration Manager (VCM) のデータ収集処理は、継続的にさらに自動化がされています。

利点

VCM の最新リリースでは、より多くのデータが自動的に収集されることに気付くため、データの収集におけるエラーや誤りが少なく、迅速な実装をもたらします。

VIPOPTS DD ステートメントにリストされている複数のライブラリーをサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して複数のライブラリーを指定する機能が追加されました。活動中のオンライン・セッションに割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに複数のライブラリーを指定する機能が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み込みます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

この機能により、複数のシステムが VIPOPTS DD ステートメント定義を共有することが可能になり、各システム用の各 VIPOPTS ライブラリーでこの情報を複製する必要はありません。

Vanguard Enforcer™

導入: Vanguard Enforcer の変更通知機能

説明

この機能で、Vanguard Enforcer の新しい機能と機能強化の成果を提供します。

利点

Vanguard Enforcer 変更通知機能は、計画目的に関して導入先を支援します。

新たしい ACEE センサー

説明

新しいセンサーは、z/OS システム内のアドレス空間に取り付けられた様々な ACEEs をスキャンします。現在、このセンサーは警告モードでのみ動作します。

利点

この ACEE センサーは、対応するセキュリティー・サーバー・プロファイル情報の内容と対立する条件について、標準の z/OS 制御ブロックに取り付けられた ACEE をスキャンします。スキャンされる情報のタイプは次の通りです：

- システム SPECIAL、システム OPERATIONS、システム AUDITOR、 ROAUDIT におけるミスマッチ
- TRUSTED 属性におけるミスマッチ
- PRIVILEGED 属性におけるミスマッチ

Vanguard Enforcer センサー開始タスクにおけるセキュリティーの改善

説明

Enforcer センサー・アドレス空間に指示できるすべてのオペレーターMODIFY コマンドは、セキュリティー・サーバー・プロファイル定義が必要です。

利点

これにより、安全対策が施されてないオペレーターMODIFY コマンドから、Enforcer センサー開始タスクのセキュリティーが改善されます。

強化された Enforcer ベースライン構築処理

説明

Vanguard Enforcer ベースライン構築処理が ISPF 環境で呼び出されると、既存のコンソール識別子と対立しないコンソール識別子が作成されます。Enforcer ベースライン構築処理の最後に、作成されたコンソール識別子は z/OS によって非アクティブとしてマークされます。

Vanguard Enforcer センサー開始タスクが初期化されると、これらの非アクティブなコンソール識別子を検索します。そのようなコンソール識別子が見つかると、z/OS サービスが呼び出されて適切な定義が削除されます。さらに、毎日午前 0 時ころに、Enforcer センサー開始タスクはこのような非アクティブな Enforcer コンソール識別子を再度検索します。

利点

この機能拡張により、非アクティブで Enforcer ベースライン構築処理と関連付けられているコンソール識別子のシステム記憶域が解放されます。

Vanguard Enforcer セキュリティー・サーバー・センサーの PASSWORD オプションのサポート

説明

Enforcer セキュリティー・サーバー・センサーが更新され、セキュリティー・サーバーの SETROPTS コマンドにより設定された IBM パスワード機能が処理されます。

利点

SETROPTS コマンドの新しい PASSWORD オプションは、セキュリティー・サーバー・センサーによりサポートされるようになりました。

Active Alerts の Vanguard Enforcer からの削除

説明

Enforcer 製品の Active Alerts 機能の将来が述べられ、Enforcer Active Alerts ECN (Enforcer 変更管理) が公表されました。このリリースの Vanguard Security Solutions で、Active Alerts 機能は Vanguard Enforcer 製品から削除されました。その代わりに、導入先は Vanguard Active Alerts 製品に移行する必要があります。

利点

この機能拡張により、どの Active Alerts 機能または製品を使用するかの導入先の選択が簡単になります。

強化された Enforcer センサーのセキュリティーと整合性

説明

多岐にわたる変更：

- Vanguard Enforcer センサー開始タスクと関連付けられているベースライン・データセットは、単一の開始タスク並行起動に制限されます。すなわち、複数の Enforcer センサー開始タスク起動は、同じベースライン・データセットを使用できません。
- APF センサー処理が修正され、ベースライン定義と APF システム定義間の不一致による異常終了が解消されました。
- SOTEMP ファイルはセキュリティー・サーバー・クラス処理から除外されました。これにより、セキュリティー・サーバー情報の曝露が削減されます。Enforcer センサー開始タスクの JCL を再構築することを推奨します。
- Enforcer センサーのロード・モジュールは、100 文字を超える PARM オプションをサポートするために、IBM バインダーLONGPARM オプションを使用するようになりました。

利点

この機能拡張により、システム・センサー操作のセキュリティーと整合性が向上します。

PPT センサーの新しい設定

説明

IBM APAR OA50215 のサポート。
この IBM APAR は PPT に 2 つの新しい設定を追加しました：
NODSI_ALLOWBATCH
NOPASS_ALLOWBATCH
これらの 2 つの新しい設定は、可能性のある整合性の問題を引き起こすことを可能にします。明示的なメッセージが PPT センサーから発行されます。

利点

この追加検査により、新しい PPT オプションの追加検査と通知が提供されます。1 つまたは両方のオプションが存在すると、z/OS システムで可能性のある整合性の問題が発生する可能性があることを、通知します。

ベースライン・データセットの可変ブロック化形式のサポート

説明

ベースライン・データセットの可変ブロック化形式のサポート：

- Vanguard Enforcer ベースライン構築処理 (ISPF ダイアログ) は、可変ブロック化形式のベースライン・データセットの定義が必要になりました。
- 現在の固定ブロック化形式のベースライン・データセットを可変形式に変換するために、Vanguard サンプル・ライブラリー(VANSAMP) に REXX exec が提供されています。

- Enforcer センサー開始タスクは、導入先に変換パスを提供するために、固定または可変形式のベースライン・データセットをサポートします。
- 可変形式のベースライン・データセットへの変更は、実際のデータセットのサイズを約 40 パーセント縮小できます。ベースライン・データセットのアクセスが若干向上します（恐らく導入先でははっきりしません）。
- この形式変更により、最大の一般リソース・プロファイル名のサイズ (246 文字) の最終的なサポートがされます。
- この形式変更により、UNIX パスとファイル名 (1024 文字) を扱う最終的なサポートがされます。
- 共用ファイル・アクセス・ルーチンの使用により、Enforcer センサー・アドレス空間内の 2GB 境界より上に、ある時点で、メンバーのキャッシングが可能になります。

利点

この機能拡張による利点は次の通りです：

- ベースライン・メンバーとレコードの共通アクセス。
- ベースライン・データセットのサイズの縮小。
- 長いプロファイル名と UNIX パスとプロファイル名を扱う将来の変更をサポート。

Vanguard ez/Integrator™

Vanguard ez/Integrator における DNS 名のサポート

説明

IP アドレスの代わりに DNS 名を使用できます。

利点

ez/Integrator の設定で DNS を指定できるようになり、静的 IP アドレスを必要とせずに、動的 IP アドレスとファイヤー・ウォールを使用できるようになりました。

Vanguard ez/Integrator における IPv6 のサポート

説明

IPv6 のサポート。

利点 s:

すべての非メインフレーム・エンティティーとの通信のために IPv6 サポートが追加されました。

Vanguard ez/SignOn™

サポートされているプラットフォーム間でパスワードを同期させる機能

説明

Vanguard ez/Signon と Vanguard Authenticator のライセンスを持つお客様は、 メインフレームの z/OS RACF、Microsoft Windows、iSeries または Linux のパスワード変更を行い、すべてのプラットフォーム間でパスワードを同期させることができます。さらに、1 つのシステムでリボークされたユーザーは他のシステムへ伝搬されます。

利点

この機能拡張により、システム間でのリボーク/ロックアウト機能を備えた、使いやすいパスワード・ソリューションをプラットフォーム間で利用できます。この機能拡張により、完全に異なるシステム間で単一のパスワード・ソリューションが可能になります。さらに、1 つのシステムでアクセスを削除したユーザーは、人の介入なしに、すべてのシステムで認証アクセスが確実に削除されます。

Vanguard ez/PIV Card™

アプリケーションの INCLUDE と EXCLUDE ジョブ名のマスキングのサポート

説明

INCLUDE/EXCLUDE ジョブ名サポートのマスキングが強化されました。

利点

ユーザーは、アプリケーションのマスキングに完全な INCLUDE と EXCLUDE サポートを使用できるようになりました。この機能拡張により、多要素認証で実施されるアプリケーションの非常に細かいまたは大まかな包含および/または除外が可能になります。

Vanguard FASTEXIT 処理の導入

説明

パフォーマンス向上が、Vanguard ez/Token のすべてのユーザーのために追加されまそた。

利点

管理者は、すべての多要素認証 (MFA) 活動からすぐに終了するユーザーの集まりを作成したり、MFA を通してのみ認証するユーザーや MFA 処理からすぐに終了する他のすべてのユーザーを設定することができるようになりました。MFA を実施しない認証を行う多数のトランザクションを持つお客様は、CPU の使用を削減することで顕著な影響を受けます。すべてのお客様は、この機能拡張により恩恵を受けることができます。FASTEXIT の設定の詳細については、該当する Vanguard MFA 製品のマニュアルを参照してください。

Vanguard ez/PIV Card における AES265 による暗号化パスワードのサポート

説明

Vanguard ez/PivCard における IBM APAR OA43999 のサポート。

利点

Vanguard 製品は、IBM z/OS の変更に基づいて継続的に更新されます。z/OS の OA43999 により、ユーザーが AES265 による暗号化パスワードを持てるようになりました。PivCard はこの環境をサポートします。Vanguard は、IBM の新機能およびリリースとの互換性を保つために、自社製品を継続的に更新することを 表明しています。

パスコード有効期限のカストマイズが Vanguard ez/PIV Card で利用可能

説明

Vanguard ez/PivCard パスコードのお客様による制御可能なタイムアウト値のサポート。

利点

以前は、Vanguard ez/PivCard パスコードは特定の時間（約 10 分）が経つ失効しました。この機能拡張により、お客様は最大 60 分までパスコードを再利用し再生できる時間間隔を指定できます。この更新により、お客様は複数のパスコードを生成することなく、Vanguard ez/PivCard と共にシームレスにセッション管理を使用できます。

Vanguard Active Alerts の SIEM 統合

説明

レポートの目的のために、成功または失敗したログオンに関する SMF レコードを作成します。レポートとセキュリティー情報とイベント管理 (SIEM) の統合をサポートするために、より多くのログの記録を追加しました。

利点

この機能の使用により、成功したログオン、失敗したログオン、多要素認証を迂回したログオン、および多要素認証を通してアクセスしなかったユーザーを追跡することにより、対象システムのユーザー認証を監査できます。この機能拡張により、Vanguard Active Alerts を通して Vanguard ez/Token との SIEM 統合も可能になり、ユーザーが間違ったログオンや連続して非常に多くの間違ったログオンを試みた場合に、即時に通知することができます。

Vanguard ez/PIV Card における通信と証明書問題の改善された診断

説明

Vanguard ez/PivCard の OCSP と CRL 処理中に、さらに多くのログの記録が追加されました。

利点

Vanguard は、オンライン認証状況プロトコル (OCSP) および証明書失効リスト (CRL) 処理中

に、さらに多くのログの記録を追加し、そのため、エンド・ユーザーが、何時認証が失敗したか、何故失敗したか、およびそれぞれのタイミングをよりよく判断できるようにしました。この更新は、Vanguard ez/PivCard の問題、および通信と証明書の問題に関する問題の診断に役立ちます。

改善されたサポートと追加の第 508 条順守

説明

マルチ・カード・リーダー、ドメインネーム・サーバー (DNS)、およびタイム・サーバーのサポートが拡張され、第 508 条アクセシビリティー・プログラム基準に準拠するためのナレーションのサポートが追加されました。

利点

マルチ・カード・リーダーが設置されている場合、特定のカードを検出し使用する能力を追加しました。より良いタイム・サーバーのサポートおよび第 508 条アクセシビリティー・プログラム基準の順守のアナウンスを使用する能力を追加しました。

Vanguard ez/PIV Card における FIPS および JAWS のサポートの追加

説明

FIPS および JAWS のサポート。

利点

第 508 条アクセシビリティー・プログラム基準をさらに順守するために、連邦情報処理規格 (FIPS) のサポートおよび音声によるジョブ・アクセス (JAWS) と呼ぶ特定のナレーション・サポートに関するサポートを追加しました。

Vanguard ez/PIV Card における DNS 名のサポート

説明

IP アドレスの代わりに DNS 名を使用できるようにします。

利点

Vanguard ez/Integrator を設定する際に DNS を指定できるようになりました。このことにより、静的 IP アドレスを必要とせずに動的 IP アドレスとファイア・ウォールを使用できます。

Vanguard ez/PIV Card における IPv6 サポート

説明

IPv6 サポート。

利点

Vanguard ez/PIV Card で使用される、タイム・サーバーや OCSP/CRL 検査を含むすべての非メイ

ンフレーム・エンティティーへの通信に IPv6 サポートを追加しました。

Vanguard ez/Token™

Vanguard 多要素認証は、セッション管理とエンタープライズ認証をサポートするようになりました。

説明

Vanguard 多要素認証 (MFA) は、セッション管理とエンタープライズ認証と一体になって機能するように強化されました。このソリューションでは、ユーザーは MFA 認証情報を使用して VTAM アプリケーションを経由して認証します。認証に成功すると、ユーザーは、同じ VTAM セッションを経由してログオンしている間は、MFA 認証情報を再度入力することなしに他のセッションを認証できます。

利点

このソリューションは、MFA 対応のユーザーがエンタープライズ・システムにアクセスするために適切に認証されていることをまだ保証している間に、そのカバーのもとでパスチケットを使用せずにセッション・マネージャーを経由してワンタイム・パスワード (OTP) 認証情報を再生するという脅威を解決します。この方法により、一度セッション・マネージャーにユーザーを認証するために、セッション管理と二要素認証 (2FA) を一緒に途切れなく使用できます。セッション・マネージャーはユーザーが認証情報を再度入力することを要求せずに、企業内の他のシステムに認証情報を渡します。

セッション・マネージャーは、導入先でこの新しい認証メカニズムを使用するための前提条件ではありません。Vanguard VTAM アプリケーションを経由して一度エンド・ユーザーに強制的にエンタープライズ認証を提供し、それから、最初の VTAM セッションがまだアクティブであれば、ユーザーはその後 RACF 認証情報だけで他のシステムに対して認証できます。

IBM 出口 IRRSXT00 への修正のサポート

説明

IRRSXT00 出口のサポートが追加されました。

利点

IBM は認証のために CICS により使用される方法を修正しました。この機能拡張により IRRSXT00 出口のサポートが追加され、それにより CICS における多要素認証の実施が可能になります。

Vanguard Active Alerts との SIEM 統合

説明

レポート処理の目的のために、成功および失敗したログオンに関する SMF レコードを作成します。レポート処理とセキュリティー情報とイベント管理 (SIEM) の統合のためにより多くのログ

の記録を追加しました。

利点

この機能拡張により、成功したログオン、失敗したログオン、多要素認証を迂回したログオン、および多要素認証を通してアクセスしなかったユーザーを追跡することにより、対象システムのユーザー認証を監査できます。この機能拡張により、Vanguard Active Alerts を通して Vanguard ez/Token との SIEM 統合も可能になり、ユーザーが間違ったログオンや連続して非常に多くの間違ったログオンを試みた場合に、即時に通知することができます。

Vanguard ez/Token による RSA 8.x サポート

説明

Vanguard ez/Token は RSA 8.x をサポートするようになりました。

利点

Vanguard 製品は、他のベンダーの新しいリリースおよび変更に基づいて継続的に更新されています。

Vanguard ez/Token による RSA SecurID に関する RACF パスワードのサポート

説明

RSA SecurID®認証に関する新しい機能を追加しました。トークン/ PIN を入手するために満了したパスワードを使用することに対比して、一つのエントリーのパスワード・フレーズ欄にパスワード/トークンまたはパスワード/トークン＋PIN が提供されます。

利点

この機能拡張により、次のいずれかをパスワード欄に入力し、Vanguard ez/Token およびバックエンド認証サーバーの設定に基づいて、すべて正しく認証されるようになります。管理者は、一つのパスワード欄入力に、RACF パスワードおよびトークンまたは PIN + トークンすべての使用を強制できるようになりました。これにより、セキュリティー強化と情報入力の手間を軽減できます。

この機能拡張の前は、ユーザーはトークンまたはトークンと PIN を入力できましたが、パスワードを入力することはできず、PIN + トークン認証を成し遂げるために新しいパスワード欄を使用する必要がありました。今ではユーザーは、単一欄にすべての必要な情報を入力し、RACF パスワード・サポートを使って認証を成し遂げることができるようになりました。

Vanguard ez/Token による ActivID 7.2 のサポート

説明

Vanguard ez/Token は ActivID v7.2.x をサポートするようになりました。

利点

Vanguard 製品は、他のベンダーの新しいリリースおよび変更に基づいて継続的に更新されていま

す。

Vanguard ez/Token による LinOTP 認証のサポート

説明

LinOTP のサポートが追加されました。

利点

Vanguard ez/Token は、YUBKEY、OATH および他のトークンと共に使用するために、バックエンド認証サーバーとして LinOTP を使用できるようになりました 。この機能拡張により、LinOTP を使用しているお客様は、z/OS メインフレーム上で実行されているあらゆるアプリケーションと共に使用するために、既存のバックエンド多要素認証サーバーを活用できます。これにより、ユーザー認証のために優れたセキュリティーが提供されます。

Vanguard ez/Token による DUO 認証のサポート

説明

Duo は、認証のためにサポートされるバックエンド・サーバーになりました。

利点

MFA のためのバックエンド認証サーバーとして、現在 DUO を使用しているか、それとも DUO の使用を検討しているお客様は、認証のための MFA として Vanguard ez/Token を使用できるようになりました。Vanguard ez/Token は仲介サービスを必要とせずにメインフレームから直接、DUO を完全にサポートします。ユーザーは、必要や状況のいずれかに応じて、スワイプ方式、パスコード方式のいずれかを使用して、DUO でログインすることができます。実装されている場合に正常にログオンするためには、ユーザーは RACF パスワードと DUO 認証を使用する必要があります。

Vanguard ez/Token による Ping Identity 認証のサポート

説明

Vanguard ez/Token は、認証のためのサポートされるバックエンド・サーバーとして、Ping Identity®認証をサポートするようになりました。

利点

MFA のためのバックエンド認証サーバーとして、現在 PingID を使用しているか、それとも PingID の使用を検討しているお客様は、認証のための MFA として Vanguard ez/Token を使用できるようになりました。Vanguard ez/Token は仲介サービスを必要とせずにメインフレームから直接、PingID を完全にサポートします。ユーザーは、必要や状況のいずれかに応じて、スワイプ方式、パスコード方式のいずれかを使用して、PingID でログインすることができます。実装されている場合に正常にログオンするためには、ユーザーは RACF パスワードと PingID 認証を使用する必要があります。

アプリケーションの INCLUDE と EXCLUDE ジョブ名のマスキングのサポート

説明

INCLUDE/EXCLUDE ジョブ名サポートのマスキングが強化されました。

利点

ユーザーは、アプリケーションのマスキングで完全な INCLUDE と EXCLUDE サポートを使用できるようになりました。この機能拡張により、多要素認証で強制されるアプリケーションの非常に細かいまたは大まかな、包含と除外の両方またはいずれか一方が可能になります。

Vanguard FASTEXIT 処理の導入

説明

すべてのユーザーのために、Vanguard ez/Token にパフォーマンスの改善が追加されました。

利点

管理者は、すべての多要素認証 (MFA) 活動からすぐに終了するユーザーの集まりを作成すること、または MFA を通してのみ認証するユーザーや MFA 処理からすぐに終了する他のすべてのユーザーを設定することができるようになりました。MFA を実施しない認証を行う多数のトランザクションを持つお客様は、CPU の使用を削減することで顕著な影響を受けます。すべてのお客様は、この機能拡張により恩恵を受けることができます。FASTEXIT の設定の詳細については、適切な Vanguard MFA 製品のマニュアルを参照してください。

ホスト・フェイルオーバー・サポートの追加

説明

ホスト・ポートのフェイルオーバーの機能拡張。

利点

Vanguard は、Vanguard ez/Token の構成にタイマー設定を追加しました。タイマー設定は応答しないホストを検出し、Vanguard ez/Token が長い待ちを強要されることなしに、次のホストに継続できるようにします。

Vanguard Offline™

VIPOPTS DD ステートメントにリストされた複数ライブラリーのサポート

説明

バッチ JCL プロシージャーの VIPOPTS DD ステートメントを通して、複数のライブラリーを指定する能力が追加されました。アクティブなオンライン・セッションで割り振られている VIPOPTS ライブラリー名の VANLIBS メンバーに、複数ライブラリーを指定する能力が含まれています。バッチ JCL は、指定されたすべてのライブラリーを VIPOPTS DD 連結に自動的に組み入れま

す。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、および Vanguard Cleanup に適用されます。

利点

これにより、各システムに対して一つ一つの VIPOPTS ライブラリーのこの情報を複製する必要なしに、複数システムが VIPOPTS DD ステートメント定義を共有することが可能になります。

Vanguard Offline レポートに印刷と電子メール機能の追加

説明

Vanguard Offline の Access History レポートと Impact Analysis レポートに印刷と電子メール機能が追加されました。

利点

レポートが必要なたびに再作成することなく、レポートを共有または保管することができます。

レポートに追加されたマスキングと新しい出力形式

説明

Vanguard Access History と Vanguard Impact Analysis レポートに、より多くのマスキングと新しい出力形式が追加されました。

利点

この機能拡張により、Vanguard Access History レポートおよび Vanguard Impact Analysis レポート処理オプションの両方で、エンド・ユーザーのニーズに対して迅速、簡単に、そしてより具体的にレポート処理を行います。

VRA Extract と Vanguard Offline 製品の互換性検査を追加

説明

1. 内部 I/O パフォーマンスとメッセージ生成の改善。
2. VRA Extract ファイルと Vanguard Offline 製品の互換性検査が追加されました。

利点

互換性検査で、Vanguard Offline 製品が VRA Extract ファイル内のデータを完全に活用することを確認し、正確なレポート処理を受け取ることを確実にします。

複数のヒストリー・マスター・ファイルをレポート処理の入力として指定する能力

説明

レポート処理の入力として、複数のヒストリー・マスター・ファイルを指定できるようになりました。

利点

この機能拡張により、Vanguard Offline 製品は、複数の異なるヒストリー・マスター・ファイルをレポート処理の入力として使用することができます。この機能拡張により、ユーザーは、一回の実行でありとあらゆるレポートを、一つまたは異なる RACF データベースに対する複数の LPAR にまたがって、レポートすることができます。この機能拡張により、複数のシステムにまたがって、レポート処理とコマンド検査を行います。

強化されたオンライン・レポート

説明

影響分析レポートの機能拡張 - オンラインおよび対象の影響分析レポート：

1. アクセス決定が使用される場合、グループ別クラス・プロファイルとメンバー情報がサポートされます。
2. FASTAUTH は、Auth カラムの下で、FAST としてサポートされます。これは、RACROUTE REQUEST=FASTAUTH によって、アクセス検査が行われたことを示します。

利点

1. 一部のオンライン・レポートで、メンバー・クラスをグループ化するために CLASS、プロファイルおよび ADDMEM を含めることができます。
2. アクセス決定がなされた場所に関するより正確な情報を提供します。

完全修飾リソースおよびプロファイル名のサポート

説明

アクセス履歴および影響分析レポートで、アクセス履歴およびプロファイル名を引用符で囲むことができます。

利点

この機能拡張により、Vanguard Offline レポート処理機能で完全修飾リソースおよびプロファイルの両方を指定することができます。以前は、ユーザーは特定のプロファイルまたはリソースに関心を持たないと想定されていたため、マスクされた値のみが許可されていました。しかしこの変更で、ユーザーは完全修飾値を指定できるようになりました。

追加の VOF 履歴ファイル・レコードの妥当性検査の追加

説明

追加の VOF 履歴ファイル・レコードの妥当性検査を追加する機能拡張。

利点

VOF 履歴ファイルがサポートされているバージョンであることを検証し、ユーザーがサポートされなくなった古いデータまたは付属物を、気付かずに提供することを防ぎます。古いデータを最新の状態にして履歴マスター・ファイルの全体的なサイズと I/O を削減する変換ユーティリティーを実行するためのメッセージをユーザーに返します。

RACFVARS サポートの追加

説明

この機能拡張により、RACF コマンドの処理時およびアクセス権限検査時の、RACFVARS プロファイルのサポートが実装されます。

利点

より正確なアクセス権限検査を可能にし、そしてリソースとアクセス検査に関するプロファイルに RACFVARS 変数を含めることを自動化します。

新しいマスキング・フィルターの追加

説明

新しい VCL および VOF フィルターが追加されました。それらのフィルターはフィルターされ取り除かれるリソースの細かさを提供します。

利点

新しいマスキング・フィルターが追加され、フィルタリング獲得中に、より具体的な細かい指定が可能になりました。

この機能拡張により、お客様は、収集のために望ましくないデータにフィルターをかける指定ができます。それは通常、Vanguard Offline と Vanguard Cleanup によって収集される膨大な量のデータです。時々、このデータは重複し、収集の目的で重要ではありません。

アクセス履歴レポートと影響分析レポートのバッチ処理のサポート

説明

この機能拡張により、Vanguard Offline の Vanguard アクセス履歴と影響分析レポートのバッチ処理が実装されます。これにより、お客様は、継続的にレポート処理をセットアップし実行することが容易になり、TSO セッションを解放し、同時にレポート処理の自動化を可能にします。

利点

より正確なアクセス権限検査を可能にします。これにより、お客様は、継続的にレポート処理をセットアップし実行することが容易になり、TSO セッションを解放し、同時にレポート処理の自動化を可能にします。

Vanguard PasswordReset™

Vanguard PasswordReset の RACF パスワード・フレーズのサポート

説明

RACF パスワード・フレーズのサポート。

利点

RACF パスワード・フレーズは、Vanguard PasswordReset で完全にサポートされるようになりました。

Vanguard PasswordReset ヘルプの更新

説明

ウェブサイトのヘルプが更新され、ページのフィールドについて説明しています。

利点

ウェブサイト上でフィールドを使用する方法を明確にしています。

Vanguard PasswordReset の USS 版 Apache のサポート

説明

USS 版の Apache のサポートを追加しました。

利点

Vanguard 製品は、最新の IBM z/OS リリースを維持するために継続的に更新されます。IBM は USS の最新リリースで Apache に切り替えたため、Apache のサポートを追加しました。

Vanguard Policy Manager™

新しいベスト・プラクティス・ポリシー： $HLQ.Policy

説明

$HLQ ポリシーの機能拡張。ユーザーが自分のデータセット・プロファイルを操作できないようにすることに加え、他人のデータセットを操作することを防ぐことができます。

利点

自身のデータセットに対する権限を持つユーザーが、既存のポリシーを変更することを防止することにより、ベスト・プラクティスのセキュリティーを簡単に実施できます。監査者とセキュリティー管理者は、この機能に関心があります。なぜなら、権限のあるユーザーによるデータの共有の拡散を防ぐためです。

新しいベスト・プラクティス・ポリシー：BP.USE.DATA.FROM.MODEL

説明

事前定義されたベスト・プラクティス、BP.USE.DATA.FROM.MODEL という名前の新しいベスト・プラクティス・ポリシーが追加されました。

アクティブの場合、VPM はモデル・プロファイルから関連データを抽出し、入力コマンドに挿

入し、FROM オペランドが指定されている場合はコマンドを再検証します。

アクティブな場合、以下のベスト・プラクティスはデータ抽出を引き起こします：

- BP.INSTALLATION.DATA.REQUIRED
- BP.OWNER.EQUALS.DATASET.HLQ
- BP.OWNER.MUST.BE.GROUP
- BP.OWNER.REQUIRED
- BP.UACC.NONE.REQUIRED

利点

特定のコマンド・プロファイルを定義する必要なしに、ベスト・プラクティス・ポリシーを入力コマンドに適用できるようにします。

新機能：コマンド監査トレイル

説明

コマンド監査トレイルという新機能が追加されました。

利点

コマンド監査トレイル・レポートは、RACF コマンドのトラッキングを提供する Policy Manager の新機能です。その新機能は、プロファイル（ユーザー、グループ、データセット、一般リソースまたは Set RACF オプション SETR）に対して実行された各 RACF コマンドを記録し、抽出処理かオンライン処理のどちらか一方を介して、単一レポートで実行されたコマンドのすべてをレポートします。

この機能によって、管理者は最近の 99 回までのすべてのプロファイルへの変更を、単一レポートで確認することができます。

この機能は、管理者が、変更を見つけて検証し、誰がその変更を実施したか何時その変更が実施されたかを識別するために使用できます。この機能は、監査者にとっても優れています。なぜなら管理者が作成したすべてのコマンドを正確に追跡して検証できるためです。この機能拡張により、RACF データベース全体の変更のすべてをレポートできます。

新しいコマンド・ポリシー：**$NOMODIFY**

説明

追加された新しいポリシー '$NOMODIFY' により、グループ・プロファイルを変更（追加、変更、削除）から保護する、ユーザーID が変更の対象プロファイルまたはパラメーターの値に使用されることを禁止する、またはグループ内のすべてのユーザーが、変更のタイプごとにわずか 1 つを使用して、変更の対象プロファイルまたはパラメーターの値に使用されることを禁止することができます。

利点

この新しいポリシーを使用して、RACF 管理者を含む誰でも変更してはならないユーザーやグループの望ましくない変更を防止できます。この機能拡張は、お客様からの要望により行われました。お客様は、ターミネーション・グループに接続されているユーザーの変更を防止することを

望み、ヘルプ・デスク管理者が再開すべきでないユーザーを再開することを防止するための方法を必要としていました。

ROAUDIT ユーザー属性のサポート

説明

ROAUDIT ユーザー属性をサポートするために次のベスト・プラクティスが追加されました。

1. BP.ROAUDIT.RESTRICTED
2. BP.AUDITOR.ROAUDIT.MUTUALLY.EXCLUSIVE

利点

1. ユーザーがシステム ROAUDIT 属性を割り当て、削除することを防ぎます。
2. ユーザーがシステム AUDITOR とシステム ROAUDIT 属性の両方をユーザーID に割り当てることを防ぎます。ユーザーが AUDITOR を所有し ROAUDIT を取得していない場合、AUDITOR 属性は自動的に止まり、その逆も同様です。

Vanguard QuickGen™

次の QuickGen の機能拡張は、Vanguard Administrator、Vanguard Advisor、 Vanguard Analyzer、Vanguard Offline、Vanguard Cleanup および Vanguard Configuration Manager に適用されます。

最初の QG フォーマットを選択する能力

説明

QG インターフェイスにオプションが追加され、ユーザーは新しい QG フォーマットか最初の QG フォーマットを選択できます。

この更新は、Vanguard Administrator、Vanguard Advisor、Vanguard Analyzer、 Vanguard Offline、Vanguard Cleanup および Vanguard Configuration Manager に適用されます。

利点

QG テンプレート・パターンの一時的な定義と実行が可能な最初の QG 機能を好むユーザーがいるかもしれません。新しい QG フォーマットは、すべてのテンプレート定義を実行前に保存する必要があります。

QuickGen の新しいタグ：FLDEXIT

説明

FLDEXIT は、QuickGen の CSV タグの下にネストされたタグとして使用できるようになりました。

利点

FLDEXIT は、CSV タグのネストされたタグとして使用できるようになりました。この機能拡張により、お客様はプログラム出口で値とフィールド名を操作できます。そして、QuickGen レポート

中にデータを独自の仕様にカスタマイズすることができます。

QuickGen の新しいタグ：SORT

説明

QuickGen に SORT タグが追加。

利点

QuickGen ユーザーが、サポートがソートされる実際のフィールドを指定できるようになりました。

この機能拡張により、お客様は QuickGen レポートの出力のソートを変更できます。従って、データ表示の観点からより多くのオプションを提供しています。

Vanguard SecurityCenter™

IDIDMAP のサポート

説明

IDIDMAP のサポートが追加。

利点

Vanguard は、IBM の新しいリリースで登場する新しいクラスと機能拡張のサポートを継続して追加しています。

SETROPTS コマンドは、コマンド生成中にメンバーおよびグループ化クラスに含まれるようになりました

説明

メンバーとグループ化クラスで SETROPTS コマンドを送信します。

利点

SETROPTS コマンドは、グループ化メンバー・クラスが修正されるときに、自動的に含まれるようになりました。

特殊文字と MIXED ALL テキストのサポート

説明

パスワード・ルールのために、特殊文字と MIXED ALL text (x) の処理が追加されました。

利点

Vanguard は、IBM の新しいリリースで登場する新しいクラスと機能拡張のサポートを継続して追

加しています。

Vanguard Tokenless Authentication™

Vanguard Tokenless Authentication でブラケット文字をサポート

説明

Vanguard Tokenless Authentication (VTA) は、ブラケット文字 (< >) をサポートします。

利点

‘< >’ をサポートする新しい電子メール・サーバーで、VTTFA を使用できるようにします。

ホスト接続と負荷分散の改善

説明

最初に成功した接続をリストの先頭に移動するための、IP アドレスの並び替えが追加されました。

利点

コンタクト・リストの一番目に応答しているホストを移動することで、ホストが応答を停止した場合に、より迅速なタイムアウトが可能になります。

この機能拡張により、複数のホスト・サーバーが使用され負荷分散を支援する場合に、認証時間が促進されます。