VANGUARD
Integrity Professionals
Information Security Experts

Vanguard Security Solutions™ Suite v2.1 最新機能

Presented by

Vanguard Integrity Professionals

IBM Server Proven

Business Partner IBM

法律上の注意事項

Copyright

Trademarks

IBM, RACF, DB2, and z/OS は、米国およびその他の国のIBM社の商標または登録商標です。UNIX は米国およびその他の国のオープングループの登録商標です。
Vanguard Security Solutions, Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, Vanguard Offline, Vanguard Security Center, Vanguard ez/Token, Vanguard ez/Signon, Vanguard Enforcer, Vanguard Policy Manager, Vanguard Cleanup, Vanguard Configuration Manager, and Vanguard inCompliance は、Vanguard Integrity Professionals – Nevadaの商標です。

VSS 2.1 が利用可能になりました

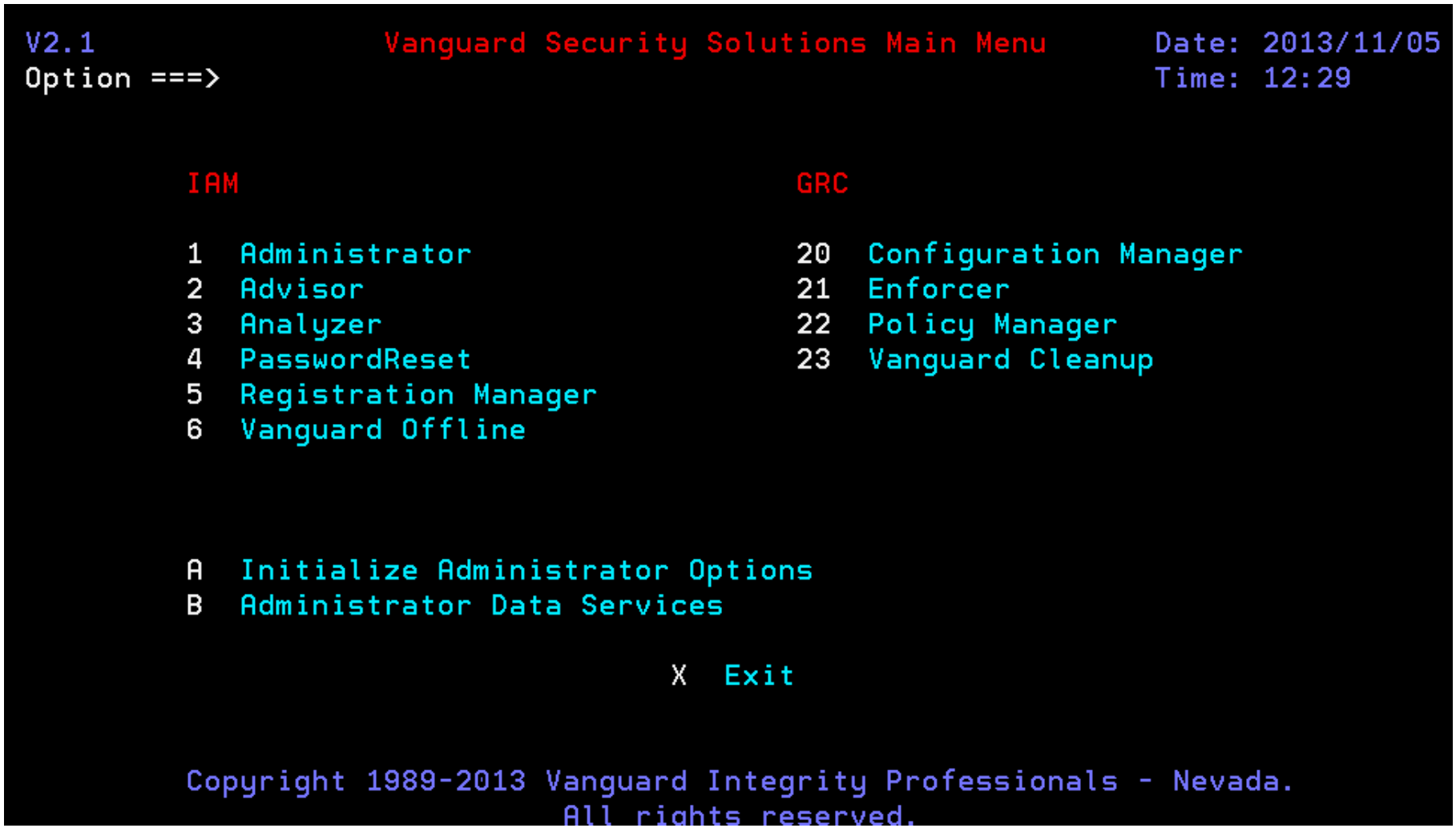
- 2013年10月米国でリリース
- 2つのソリューショングループに再編成
  - IAM (Identity and Access Management)
  - GRC (Governance, Risk, and Compliance)
- VCM (Vanguard Configuration Manager™)を標準インストール環境に統合
- 全てのライセンス製品コードを、1つのライセンスコードに統合

Identity and Access Management

VANGUARD
Integrity Professionals
Information Security Experts

- **Vanguard Administrator™**
- **Vanguard Advisor™**
- **Vanguard Analyzer™**
- **Vanguard Offline™**
- **Vanguard Security Center™**
- **Vanguard ez/Token™**
- **Vanguard ez/Signon™**

最新メインメニュー



Vanguard Administrator™

VANGUARD
Integrity Professionals
Information Security Experts

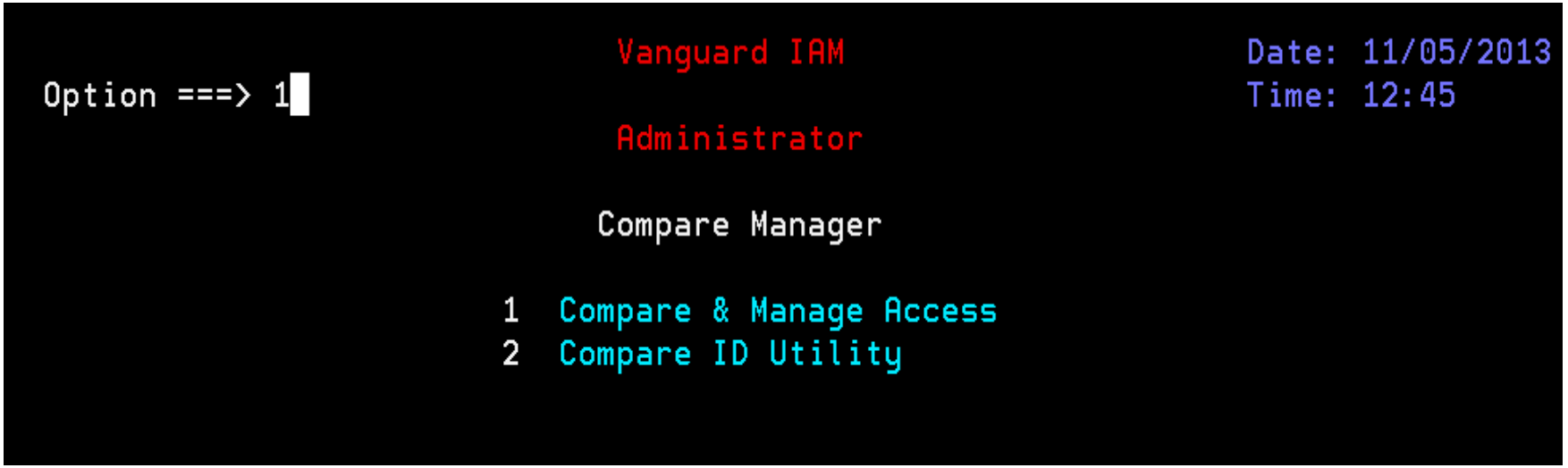
Compare Manager (option 21)

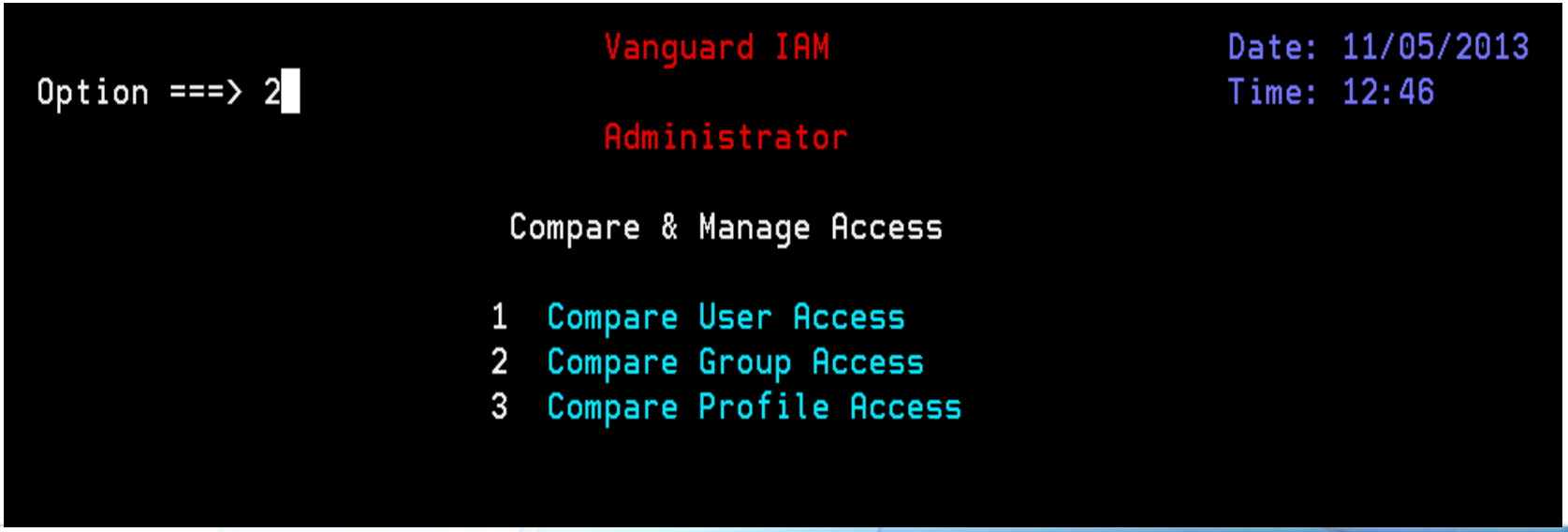
- Compare Managerでは、比較したユーザー、グループ、またはプロファイルに基づいて、違いをレポートしたり、プロファイルの違いを解消するためにプロファイル変更のコマンドを生成し、実行できます。

Vanguard Unix Manager (VUM – Option 14)

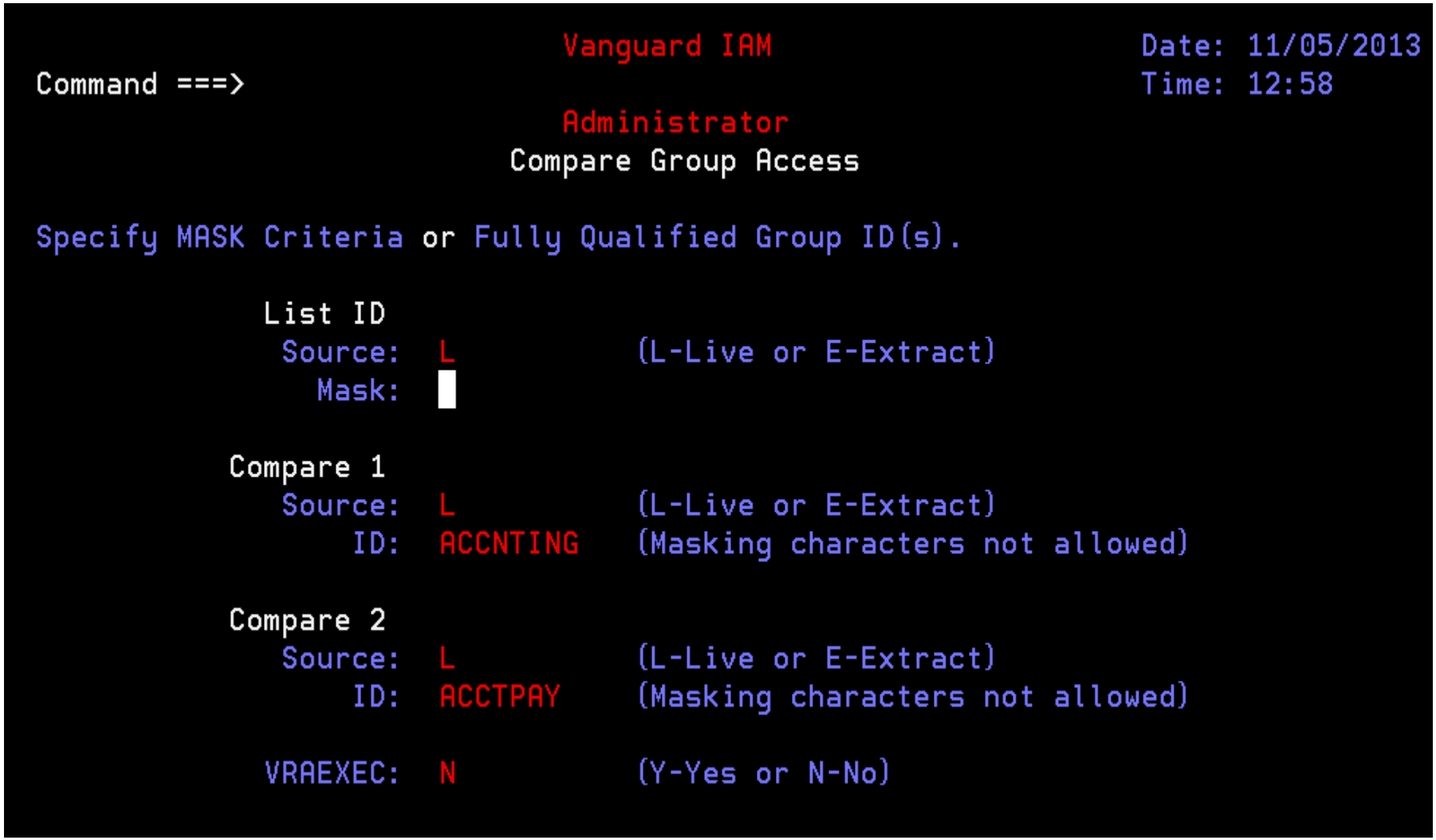
- セキュリティ管理は、UNIX® Managerを使用して、IBM®RACF®で定義されているアクセスに影響するプロファイル情報と同様に、UNIXファイルアクセスリスト、UNIXファイルシステム、UIDs およびGIDs など数多くの情報をレポートできます。

Compare Manager

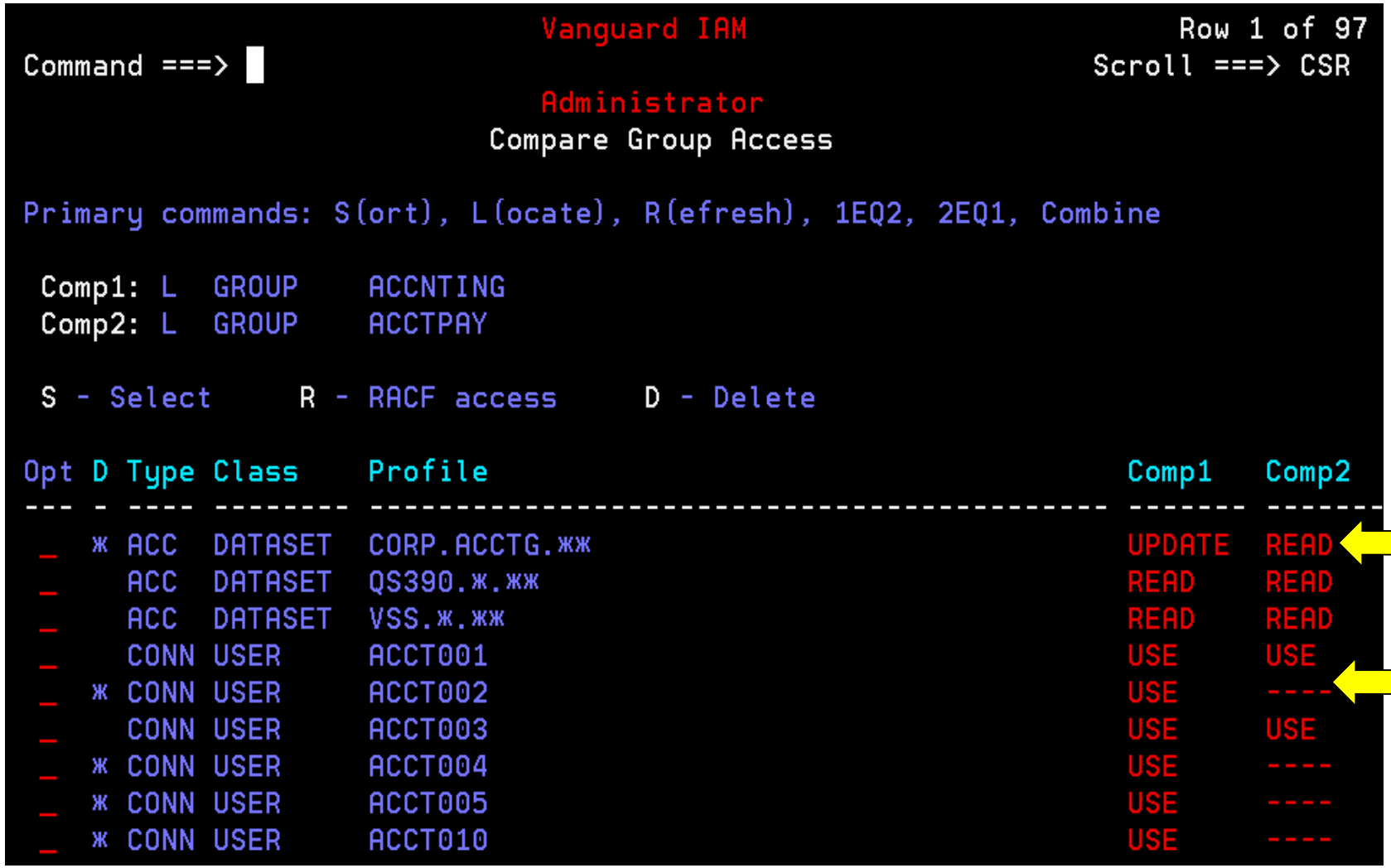




Compare Manager



Compare Manager



VUM – Vanguard Unix Manager

以下は、ライブデータや抽出ファイルを利用して実行できる、新しい機能の例です。

- 1. 所有者、グループ、またはワールド·アクセス権毎のファイルサマリー。
- 2. 所有者、グループ毎のファイルサマリー。
- 3. ファイル属性、ファイル監査ビット、ファイルのアクセス権、許可リスト内のUID、許可リスト内のGID毎のファイルサマリー。
- 4. “x” ビットオフのディレクトリー。
- 5. 壊れたシンボリックリンク。
- 6. ユーザー指定のマスキング基準毎のファイル。
- 7. UNIX®ファイルシステムのIBM Z/ OS®定義（BPXPARMS）に基づくすべての情報。
- 8. UID、PROGRAM、HOMEとSTATUSでの相互参照ユーザのリスト（ホームディレクトリがUnixに有効に定義されているかどうかを示します）。
- 9. GIDと各グループに接続しているユーザ数のリスト。
- 10. UNIXのパーミッションや能力に影響を与えるCLASSプロファイル（FACILITY、UNIXPRIV、 SURROGATおよびOPERCMDS）のリスト。

VUM –Unix Manager(Main Menu)

All new options

Same as before

VUM –Unix Security Manager(option 1)

VANGUARD
Integrity Professionals
Information Security Experts

```
Command ===>                          Vanguard IAM                  Date: 13/11/13
                                                                    Time: 13:48
                                      Administrator
                                   Unix Security Manager

                              1  File Security
                              2  File System

                              3  Owner and UID
                              4  Group and GID

                              5  FACILITY Class Profiles
                              6  UNIXPRIV Class Profiles
                              7  SURROGAT Class Profiles
                              8  OPERCMDS Class Profiles
```

VUM –Unix File System (option 2)

VANGUARD
Integrity Professionals
Information Security Experts

```
                                Vanguard IAM                          Row 1 of 21
Command ===>                                                     Scroll ===> CSR

                               Administrator
                             Unix File System

Primary commands: S(ort), L(ocate)

Next to only one entry:
 S - Select       R - RACF access

Opt  Dataset and Path                                          Mode        Type
---  ------------------------------------------------------    ----------  ----
 _   CSQ701.MQM.ZFS                                            Read Only   ZFS
          /Z112/usr/lpp/mqm/V7R0M1
 _   DFH410.JVMPROFS.ZFS                                       Read/Write  ZFS
          /Z112/usr/lpp/cicsts/cicsts41/JVMProfiles
 _   DFH410.SAMPLES.ZFS                                        Read/Write  ZFS
          /Z112/usr/lpp/cicsts/cicsts41/samples
 _   DFH410.SECURITY.ZFS                                       Read/Write  ZFS
          /Z112/usr/lpp/cicsts/cicsts41/lib/security
 _   DFH410.ZFS                                                Read Only   ZFS
          /Z112/usr/lpp/cicsts/cicsts41
 _   HFS.ADCDPL.ROOT                                           Read/Write  HFS
```

VUM –Facility class profiles(option 5)

VANGUARD
Integrity Professionals
Information Security Experts

```
                                Vanguard IAM                          Row 1 of 23
Command ===>                                                    Scroll ===> CSR

                                Administrator
                            FACILITY Class Profiles

Primary commands: S(ort), L(ocate)

Next to only one entry:
 A - Activate   D - Delete   S - Select   R - RACF access

Opt  Status     Profile                                                 UACC
---  --------   ------------------------------------------------------  -------
 _   Active     BPX.DAEMON                                              NONE
 _   Active     BPX.DAEMON.HFSCTL                                       NONE
 _   Active     BPX.DEFAULT.USER                                        NONE
 _   Active     BPX.NEXT.USER                                           NONE
 _   Active     BPX.SERVER                                              NONE
 _   Active     BPX.SUPERUSER                                           NONE
 _   Active     BPX.UNIQUE.USER                                         NONE
 _   Active     BPX.WLMSERVER                                           NONE
 _   Inactive   BPX.CF
 _   Inactive   BPX.CONSOLE
 _   Inactive   BPX.DEBUG
```

VUM –Surrogat class profiles(option 7)

VANGUARD Integrity Professionals
Information Security Experts

```
                                Vanguard IAM                          Row 1 of 7
Command ===>                                                  Scroll ===> CSR

                                Administrator
                            SURROGAT Class Profiles

Primary commands: S(ort), L(ocate)

Next to only one entry:
 A - Activate   D - Delete   S - Select   R - RACF access

Opt  Status     Profile                                                UACC
---  --------   ----------------------------------------------------   -------
 _   Active     BPX.SRV.INTERNAL                                       NONE
 _   Active     BPX.SRV.PKISERV                                        NONE
 _   Active     BPX.SRV.PRIVATE                                        NONE
 _   Active     BPX.SRV.PUBLIC                                         NONE
 _   Active     BPX.SRV.WEBADM                                         NONE
 _   Active     BPX.SUBMIT.OPE                                         NONE
 _   Inactive   BPX.SRV.*
**************************** Bottom of data ****************************
```

Vanguard Administrator™ その他の機能強化

VANGUARD Integrity Professionals
Information Security Experts

使用できないプロファイルサマリー

このレポートは、プロファイル名に総称文字(*, %)を持っているが、総称文字を利用できないクラス(NOGENCMD または NOGENERIC)に定義されている個別一般資源プロファイルをリストします。
注意: NOGENERICのレポートおよびコマンド生成は、RACF V1R12以上が必要です。

デジタル証明書の有効期限レポート拡張

レポート形式は、読み易くするために、デジタル証明書のデータが含まれるように拡張されました。

マスキングのリテラルとして可能な総称文字

例: **'SYS1.*.**'**

Quickgen 拡張

抽出統計データのレポート
新キーワード: SKIPALLBLANKS（空白除去）

DB2® V10 サポート追加

Vanguard Advisor™

VANGUARD
Integrity Professionals
Information Security Experts

Advisor 抽出ファイルのIDCAMS REPRO出力をバッチレポートの入力として利用可能

ADVISOR 抽出ファイルのIDCAMS REPRO出力をバッチレポートの入力として指定可能になりました。VSRR DD文で複数ファイルを指定可能です。

UNIX System Services マスキングパラメータのサポート追加

サマリおよび詳細レポートで、9個の項目に対してマスキング指定が可能。
実効GID, 実効UID, 実GID, 実UID, 保存GID, 保存UID, スーパーユーザ, ユーザセキュリティトークン, BPX.DEFAULT.USER

レポート中に最古と最新のレコードを出力

入力ソースがSMFファイルの場合、バッチレポートの最後に入力レコードの最古と最新の日付と時間を出力します。(FROM～TO)

アクティブアラートEメール強化

アクティブアラートメールの種類毎に独自の件名を指定できるようになりました。件名は60文字以内でシステム上の記号パラメータ(例えば、リアルタイム通知が稼働しているSMFID(&SYSSMFID))を含める事が可能になりました。

ヘルプパネルにオプションRTが追加

ヘルプパネルにAdvisorレポートとSMFタイプの関係（どのレポートを出力するにはどのSMFタイプが必要か）が簡単に確認可能となるようにRTオプションが追加されました。

Unix System Services レポートが強化

イベントコード 67(initACEE), イベント修飾コード 09 と 10 およびイベントコード 69(RPKIGENC), イベント修飾コード 08 と 09が追加

システムエントリーレポートが強化

イベントコード 01, イベント修飾コード 39 が追加（分散型IDに対するRACFユーザIDは発見できない）

DB2 圧縮 SMF レコードをサポート

DB2 V10 からレコード格納に必要なスペース容量を減少させる目的で、SMFタイプ100-102レコードの圧縮が開始されました。AdvisorはDB2サマリーおよび詳細レポートにSMFタイプ102を使用しており、新しい形式に対応しました。

PDS/E サポート

AUDITSETROPTS 強化

レポート生成で以下の2つのオプションが利用可能:

Exceptions only ===> YES
Class Detail ===> YES

例外のみ(Exceptions only)

オプションデータセットのVSAOPT00メンバー内EXPTONLYLEVELパラメータで指定したもの以上のメッセージの重要度を持つエントリのみを一覧表示するには、[はい]を指定する

クラス詳細(Class Detail)

クラス記述子テーブル内のプロパティと、各クラスの特性をリストするには、[はい]を指定します。

Vanguard Offline™

Vanguard Offline™ は、顧客が本番RACFデータベースには影響しない環境で、RACFデータベースへの変更をテストすることができるVanguard社のIAM製品グループの新製品です。

Vanguard Offline™ は、変更後に全く意図しない結果が生じないことを事前に検証するために、テスト変更することができる製品です。

Vanguard Offline™ は、管理者がRACFプロファイルを生成、削除および変更により、すべてのユーザとグループのアクセスへの影響を確認するためにテストすることができます。（変更による影響分析が可能）

注意：この製品は、V1.13のメンテナンスレベルを上げることでも利用可能となります。

Vanguard Offline™ – 新機能

ユーザアクセス許可と拒否レポート –
(Vanguard Access History Report)

マスキングおよびquickgen機能を使用して、データセットおよび一般資源へのユーザ毎のアクセスをレポートします。この新しいレポートでは、SMFの監査を必要とせずに、データセットと一般資源に対し、アクセス許可、アクセス要求、許可されたアクセスと拒否されたアクセスの知識を得るために使用することができます。

ヒストリーマスターファイルマージ処理

RACFデータベースを共用している異なるシステムで、レポートのために後でマージできる別々のヒストリーマスターファイル（HMF）を持つことができるように、製品のより柔軟な処理を可能にします。

Vanguard Offline™


```
                                  Vanguard IAM
Command ===> 2
                          Vanguard Access History - Extract

                        1  Access Summary by Access
                        2  Access Summary by User
                        3  Access Summary by Group
                        4  Access Summary by Class
                        5  Access Summary by System
```

```
Command ===>
                                        Access Summary by User

Primary commands: S(ort), L(ocate)

Next to only one entry:
 S - Select     Q - QuickGen     V - View

Opt    User        Reqsted    Allowed    Access        Event
---    --------    -------    -------    -------    --------
 _     DOUGB       Read       None       DENIED           23
 _     DOUGB       Read       None       GRANTED           4
 _     DOUGB       Read       Read       GRANTED         412
 s     DOUGB       Read       Update     GRANTED          30
 _     DOUGB       Update     Alter      GRANTED         938
```

Vanguard Offline™

VANGUARD
Integrity Professionals
Information Security Experts

```
                                  Vanguard IAM                          Row 1 of 30
Command ===>                                                    Scroll ===> CSR
                              Access History Detail

Primary commands: Q(uickGen), V(iew), S(ort), L(ocate), SW(itch)

Next to only one entry:
 S - Select

Opt User     System  Access  Class      Resource -Reqsted(Read) Allwd(Update)
--- -------- ------- ------- ---------  ---------------------------------------
 s  DOUGB    SRV1    GRANTED DATASET    USER.LINKLIB
    DOUGB    SRV1    GRANTED DATASET    SYS1.VAN.RACFPRIM
 _  DOUGB    SRV1    GRANTED DATASET    SYS1.BRODCAST
```

```
                                  Vanguard IAM                          Row 1 of 30
                          Reqsted(Read) Allwd(Update)

                  System: SRV1                                Date: 2012/09/19

                    User: DOUGB                             Access: GRANTED
          Connect Group: VANGUARD                        Requested: Read
                   Class: DATASET                          Allowed: Update

                Resource: USER.LINKLIB

             Auth Profile: USER.LINKLIB


 _  DOUGB    SRV1    GRANTED DATASET    QWI.R740.QWIPNL
```

Governance, Risk Mgmt & Compliance

VANGUARD Integrity Professionals
Information Security Experts

- **Vanguard Enforcer™**
- **Vanguard Policy Manager™**
- **Vanguard Cleanup™**
- **Vanguard Configuration Manager™**
- **Vanguard inCompliance™**

新メインメニュー


```
V2.1                  Vanguard Security Solutions Main Menu      Date: 2013/11/05
Option ===>                                                      Time: 12:29

        IAM                                    GRC

        1  Administrator                       20  Configuration Manager
        2  Advisor                             21  Enforcer
        3  Analyzer                            22  Policy Manager
        4  PasswordReset                       23  Vanguard Cleanup
        5  Registration Manager
        6  Vanguard Offline


        A  Initialize Administrator Options
        B  Administrator Data Services

                                  X  Exit

        Copyright 1989-2013 Vanguard Integrity Professionals - Nevada.
                            All rights reserved.
```

Vanguard Cleanup™

VANGUARD
Integrity Professionals
Information Security Experts

RACFデータベースを解析し、未使用のユーザー、グループ、接続データ、データセットと一般資源プロファイルを削除するコマンドを作成する新しい製品です。

クリーンアップはRACF許可EXITを利用し、RACFデータベースの活動を捕捉する開始タスクを持っています。開始タスクでキャプチャされたイベントは、履歴レポートのためにVSAMファイルに格納されています。

顧客は、一定期間（月次、四半期、年次のすべての処理サイクルをカバーする必要があります）、顧客の環境で開始タスクとEXITを稼働します。
この製品は、RACFデータベースから、すべての未使用のユーザー、グループ、接続データ、データセットと一般資源についてのレポートや未使用プロファイルの削除コマンドを提供します。

注意: この製品は、V1.13のメンテナンスレベルを上げることで利用可能となります。

Vanguard Cleanup™ 強化

ヒストリーマスターファイルマージ処理

RACFデータベースを共用している異なるシステムで、レポートのために後でマージできる別々のヒストリーマスターファイル（HMF）を持つことができるように、製品のより柔軟な処理を可能にします。

VANOPTS中に&SYSNAME, &SYSSMFID と &SYSPLEXを使用可

Cleanup™とOffline™は、VCLOPT00でセットアップすることができるように、VROヒストリーマスターファイル、VOFヒストリーマスターファイルとログ･ストリームデータセットのプレフィックスに、静的システムシンボル（&SYSNAMEと &SYSSMFID）の指定ができるように変更されたので、単一のVCLOPT00指定で、これらのファイルの名前に衝突することなく、複数のシステム間で使用可能。

Vanguard Cleanup™ で排他メンバー使用が許可

クリーンアップ処理中にクリーンアップを除外するメンバー（ユーザー、グループ、データセット、一般的なリソースクラスおよびプロファイル）を指定することができます。

Vanguard Cleanup™ 強化

VCLOPTxx 別メンバを提供

VCLは、開始タスク起動時に特定のVCLOPTxxメンバーを指定することができます。これにより、クリーンアップ開始タスク実行中でも、各システム固有の設定を提供することができます。

DLFCLASS 仕様

DLFCLASSは、特定のリソースがDLFに配置されるべきか否かをチェックするためにRACFによって使用される。この新しい拡張機能を使用すると、DLFCLASSからのアクセス記録を無視して、それがDLFCLASS内の任意のプロファイルを整理するコマンドを生成しないことを、CLEANUP STCに指示することができます。

Vanguard Cleanup™ 強化

VANGUARD Integrity Professionals
Information Security Experts

ヒストリー収集詳細レポートが改善

NO PROFILEはアクセス要求を決定するためにRACFによって使われたように、以前はプロファイルをカバーしているエリアは空白のままでした。詳細な情報が、その状況の理由として、エンドユーザに提供されます。
アクセス値は以下の通り。

<NO PROFILE USED>
<DISCRETE PROFILE>
<INT GENERIC PROFILE>
<GENERIC PROFILE>
<GLOBAL ACC PROFILE>
<NO PROFILE FOUND>

新VERIFY/VERIFY(X) レポート

通常のユーザーログオン対VERIFY/ VERIFYX経由で認証されたユーザのレポートを提供します

Vanguard Configuration Manager™

VANGUARD Integrity Professionals
Information Security Experts

DISA STIGs バージョン 6.10 - 6.16 をサポート

VCMは、常に最新のSTIGのリリースに準拠するように更新されています。この機能拡張は、3ヶ月毎の新しいDISA STIGチェックのリリースに合わせて、常に最新状態を維持します。

RACF ユーザリストに対するグループ同期

収集したデータをRACFグループに保存すると、グループを展開し、現在のリストにグループに接続しているユーザーを保存します。
あなたがグループに入れると、そのRACFグループに加えた変更は、将来的には、データ収集に含まれます。

ACP00340 チェックの改善

ACP00340はAPF、LPAおよびProclibsに対しベースラインを利用するように変更されたため、実行の間に変更されている任意のメンバを見つけるために使用することができます。

暗号化はデータセットの拡張結果

VCMの結果ファイルは、製品の外部から誰もがデータを参照できないように、AESアルゴリズムを用いて暗号化することができます。

相互参照比較の拡張

ユーザは複数の異なるまたは類似バージョン間のDISA STIG結果ファイルを比較することができます。STIGSの異なるバージョン間、または異なる結果セットを含むSTIGSの同じバージョンに対し、実行した検査の比較ができます。

REPORTFINDINGS/REPORTNOFINDINGS

以前詳細レポートは、1回以上のチェックによって生成されたすべてのメッセージのダンプリストを提供していました。今回の変更により、確認したいメッセージのセットに基づいて、より具体的な報告を要求することができます。ユーザは問題箇所のみのメッセージ、問題の無い箇所のみのメッセージ、すべてのメッセージを取得することができます。問題箇所メッセージにのみ関心がある場合、調査結果を修正する必要がある場合、にこれが役立ちます。

COLLECTIONQUESTIONS

製品からの質問のすべてのリストを取得することができます。あなたは、すべての質問の完全なリストと質問に関連付けられているヘルプを返すバッチレポートを実行できます。

Questions