RACF® Update

New York/Tampa/Dallas/Raleigh RACF Users Group

15 May 2024

Bruce Wells, brwells@us.ibm.com

Mark Nelson, markan@us.ibm.com

Agenda

- **What's news since the last NY/Tampa/Dallas/Raleigh RACF Update?**
  - SPECIAL user password revocation prompt suppression
  - Support for AES as the password-based encryption algorithm for PKCS#12 packages in both RACF and PKI Services
  - RVARY password protection

SPECIAL User Password Revocation Prompt Suppression APAR OA63091

SPECIAL User Password Revocation Prompt

- **SETROPTS PASSWORD(REVOKE(nnn))**
  - *Establishes the maximum number of incorrect authentication attempts before a user is revoked.*

- **When an incorrect logon attempt exceeds the REVOKE limit:**
  - *Non-SPECIAL users are revoked immediately*
  - *Users with the SPECIAL attribute get a message sent to the console to ask the operator if the user should be revoked or allowed an additional attempt*

- **ICH301I MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER *userid* [AT TERMINAL *terminalid*.]**
  - ICH302D REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID *userid*.
    - Y – Allows the attempt to logon and does not revoke the user
    - N – Revokes the user

Disabling the Excessive Password Prompt

- **With OA63091 (V2.3, V2.4, V2.5) you can disable additional logon attempts for a RACF SPECIAL user once the SETROPTS PASSWORD(REVOKE(nnn)) value has been exceeded**
  - *The disablement can be enabled on an application-by-application basis*

- **Enabled with the definition of an XFACILIT class discrete profile of the name:**
  - ***IRR.DENY.SPECIAL.USER.ADDITIONAL.PASSWORD.ATTEMPTS.APPL.appl-name***
  - *The appl-name must match the APPL= value on the RACROUTE REQUEST=VERIFY.*
  - *If no appl-name was specified on the REQUEST=VERIFY, then it defaults to the same derivation method as used in PassTicket application name derivation.*
  - *This is a profile existence check only. No profile attributes (UACC, access list, etc.) are considered.*

AES support for PKCS#12 certificate packages APAR OA65002 (RACF), OA65003 (PKI Services)

Overview

- **Who (Audience)**
  - *Security administrators*
  - *Security auditors*

- **What (Solution)**
  - *Support for AES encryption using new PBE keyword of RACDCERT EXPORT*
  - *Ability to RACDCERT ADD such certificates*
  - *New configuration variable in PKI Services to specify the password encryption algorithm for exported PKCS#12 packages*

- **Wow (Benefit / Value, Need Addressed)**
  - *Compliance with NIST guidelines*
  - *Stronger security posture*
  - *Interoperation with certificates generated by other products*

Overview – RACDCERT ADD

- **Previously, an attempt to ADD (import) digital certificates from a PKCS#12 package protected with PBES2 (Password-Based Encryption Scheme 2) failed with**

```
IRRD104I The input data set does not contain a valid certificate.
```

- **Now, ADD just works. There are no new externals.**

Overview - EXPORT

```
RACDCERT EXPORT(LABEL('label-name'))
    [ ID(certificate-owner) | SITE | CERTAUTH ]
   DSN(output-data-set-name)
    [ FORMAT(
      CERTDER
       | CERTB64
       | PKCS7DER
       | PKCS7B64
       | PKCS12DER
       | PKCS12B64
      ) ]
    [ PASSWORD('pkcs12-password')] [PBE(AES)]
```

New PBE keyword

PBE(AES)

Indicates that the Password-Based Encryption Scheme 2 with Key Derivation Function 2 (PBES2 with PBKDF2) is to be used for protecting the PKCS#12 package when the export format is either PKCS12DER or PKCS12B64. When this option is specified, the PKCS#12 package is created using AES256 encryption with SHA256 hashing.

The only acceptable value for this keyword is AES.

This keyword is applicable when a password is specified on the PASSWORD keyword.

When PBE(AES) or PBE without a value is specified, the password entered must be 8 to 128 characters in length. Otherwise, the EXPORT command fails with message IRRD306I. If PBE is not specified, the PKCS#12 package is created with the default encryption algorithm (PBES1 with TDES).

PKI Services support

- **PKI Services provides an option to build the PKCS#12 package with Password Based Encryption Scheme Version 2 (PBES2)**
- **New keyword PKCS12EncryptAlg in the pkiserv.conf configuration file is provided under the CertPolicy section**
- **PKI Services creates PKCS#12 packages at the time the certificate is issued, so existing packages are unchanged.**

PKCS12 Encryption Algorithm Specification

Parameter	Information needed	Where to get this information	Sample value or your customized value
PKCS12EncryptAlg	Specifies the password-based encryption scheme algorithm to be used to protect the contents of a PKCS#12 package when PKI Services generates the public and private key pair. Acceptable values for this keyword are: 0, 1, or 2. These numbers correspond to the algorithm strings used in System SSL, as follows: • 0 - x509_alg_pbeWithSha1And3DesCbc. This is the default algorithm (PBES1 with TDES). **• 1 -x509_alg_pbes2WithSha256AndAesCbc256. Specify this value if you want to use the AES256 password-based encryption scheme (PBES2) with SHA256.** **• 2 - x509_alg_pbes2WithSha384AndAesCbc256. Specify this value if you want to use the AES256 password-based encryption scheme (PBES2) with SHA384.**	UNIX programmer decides this value.	1

RVARY Password Protection
APAR OA65905

Overview

- **Who (Audience)**
  - *Security administrators and auditors*
- **What (Solution)**
  - *Protect RVARY passwords with the KDFAES hashing algorithm (all supported releases)*
- **Wow (Benefit / Value, Need Addressed)**
  - *Meet NIST guidelines*
  - *Enhanced security posture*

KDFAES protection for RVARY passwords

- **OA65905 provides stronger protection of RVARY passwords**
- **It requires an action to change the passwords using a new KDFAES keyword of the SETROPTS RVARYPW command (see HOLD text)**
- **The action should not be performed until all system sharing the RACF database are IPLed with the PTF for OA65905**
  - *In a sharing environment, the action need only be performed once, from any one of the sharing systems*
  - *The action can be performed immediately on a non-sharing system*
- **The service will be required co-existence for z/OS Next.**

KDFAES protection for RVARY passwords

- **Today's SETROPTS LIST output:**

```
PASSWORD PROCESSING OPTIONS:
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS  30 DAYS.
  PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  NO PASSWORD HISTORY BEING MAINTAINED.
  USERIDS NOT BEING AUTOMATICALLY REVOKED.
  NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
  NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

KDFAES protection for RVARY passwords

- **After IPLing with the service:**

```
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
  KDFAES PASSWORD CONVERSION IS PENDING. (SEE APAR OA65905)
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
  KDFAES PASSWORD CONVERSION IS PENDING. (SEE APAR OA65905)
```

- **This is how you can confirm that the service is installed on a given system**

KDFAES protection for RVARY passwords

- When all sharing systems have the service, change your passwords to pick up the new KDFAES protection:

```
SETROPTS RVARYPW(SWITCH(xxxxxxxx) STATUS(yyyyyyyy) KDFAES)
```

- SETROPTS LIST now shows:

```
INSTALLATION DEFINED RVARY SWITCH KDFAES PASSWORD IS IN EFFECT.
INSTALLATION DEFINED RVARY STATUS KDFAES PASSWORD IS IN EFFECT.
```

- This is how you know that you've completed the action

KDFAES protection for RVARY passwords

- **You have entered ‘KDFAES mode’ and you never need to specify the KDFAES keyword again when changing RVARY passwords**
- **This works even if changing the password to the default (future changes to an installation-defined value will use KDFAES)**
  - *We recommend you don’t run with the default*
- **You can ‘change’ the passwords to their existing values**
  - *We recommend you take the opportunity to establish a new value*

KDFAES protection for RVARY passwords

- **Programs can use the R_admin service (IRRSEQ00) to extract SETROPTS settings**
  - *Two new fields indicate the format of the RVARY passwords*
  - As with SETROPTS LIST, R_admin (ADMN_XTR_SETR function code) can be used to detect:
    - Whether or not the service is installed
      - If new fields RVARSWFM (switch password format) and RVARSTFM (status password format) are returned, the service is applied
    - Whether or not the required action has been completed
      - If new fields RVARSWFM or RVARSTFM contain a value of “LEGACY”, the action has not been performed for that password
      - If new fields RVARSWFM or RVARSTFM contain a value of “KDFAES”, the action has been performed for that password
  - FYI, existing fields RVARSWPW and RVARSTPW (unchanged) indicate whether the password is the default (“DEFAULT") or installation-defined ("INSTLN").

RACF Update

New York/Tampa/Dallas/Raleigh RACF Users Group

15 May 2024

Bruce Wells, brwells@us.ibm.com

Mark Nelson, markan@us.ibm.com