VNF Security Requirements Update

VNF Security Requirements

VNF Requirements Jira

IAM Update for Frankfurt

Identity Lifecycle Management

NO CHANGE - Requirement: R-99174

The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, support the creation of multiple IDs so that individual accountability can be supported.

NO CHANGE - Requirement: R-75041
The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, support configurable password expiration.

NO CHANGE - Requirement: R-844011
The VNF MUST not store authentication credentials to itself in clear text or any reversible form and must use salting.

NO CHANGE - Requirement: R-46908
The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, comply with “password complexity” policy. When passwords are used, they shall be complex and shall at least meet the following password construction requirements: (1) be a minimum configurable number of characters in length, (2) include 3 of the 4 following types of characters: upper-case alphabetic, lower-case alphabetic, numeric, and special, (3) not be the same as the UserID with which they are associated or other common strings as specified by the environment, (4) not contain repeating or sequential characters or numbers, (5) not to use special characters that may have command functions, and (6) new passwords must not contain sequences of three or more characters from the previous password.

CHANGE - Requirement: R-814377 (VNFRQTS-837)
The VNF **MUST** have the capability of allowing the Operator to create, manage, and automatically provision user accounts using an Operator approved identity lifecycle management tool using a standard protocol, e.g., NETCONF API.

- Identify protocols to support
- Identify requirement specifying protocols supported by VNFs

The VNF **MUST** have the capability of allowing the Operator to create, manage, and automatically provision user accounts using using one of the protocols specified in Chapter 7.

NEW - Requirement: R-xxxxxx (VNFRQTS-817)

The VNF **MUST**, if not integrated with the operator's IAM system, provide a mechanism for assigning roles and/or permissions to an identity.

NEW - Requirement: R-xxxxxx (VNFRQTS-818)

The VNF MUST support at least the following roles: system administrator, application administrator, network function O&M.

CHANGE - Requirement: R-86835 (VNFRQTS-819)
The VNF **MUST** set the default settings for user access to deny authorization, except for a super user type of account. When a VNF is added to the network, nothing should be able to use it until the super user configures the VNF to allow other users (human and application) have access.

The VNF **MUST** set the access default settings to deny authorization, except for a super user type of account. ~~When a VNF is added to the network, nothing should be able to use it until the super user configures the VNF to allow other users (human and application) have access.~~

CHANGE - Requirement: R-931076 (VNFRQTS-820)
The VNF **MUST** support account names that contain at least A-Z, a-z, 0-9 character sets and be at least 6 characters in length.

The VNF **MUST** support account names that contain at least A-Z, a-z, and 0-9 character sets and be at least 6 characters in length.

Access Control

CHANGE - Requirement: R-42874 (VNFRQTS-822)
The VNF **MUST** allow the Operator to restrict access to protected resources based on the assigned permissions associated with an ID in order to support Least Privilege (no more privilege than required to perform job functions).

REMOVE - Requirement: R-15671 (VNFRQTS-794)
The VNF **MUST** provide access controls that allow the Operator to restrict access to VNF functions and data to authorized entities.

CHANGE - Requirement: R-23135 (VNFRQTS-821)
The VNF **MUST**, if not integrated with the Operator’s identity and access management system, authenticate all access to protected resources ~~GUIs, CLIs, and APIs~~.

REMOVE - Requirement: R-71787 (VNFRQTS-841)
Each architectural layer of the VNF (eg. operating system, network, application) **MUST** support access restriction independently of all other layers so that Segregation of Duties can be implemented.

The new requirement in VNFRQTS-818 will give an operator the capability of implementing segregation of duties.

NO CHANGE - Requirement: R-59391

The VNF **MUST NOT** allow the assumption of the permissions of another account to mask individual accountability. For example, use SUDO when a user requires elevated permissions such as root or admin.

CHANGE - Requirement: R-81147 (VNFRQTS-823)
The VNF **MUST** support strong authentication, also known as multifactor authentication, on all protected interfaces exposed by the VNF for use by human users. Strong authentication uses at least two of the three different types of authentication factors in order to prove the claimed identity of a user.

The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, support multifactor authentication on all protected interfaces exposed by the VNF for use by human users.

CHANGE - Requirement: R-79107 (VNFRQTS-824)
The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, support the ability to disable the userID after a configurable number of consecutive unsuccessful authentication attempts using the same userID.

The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, support the ability to lock out the userID after a configurable number of consecutive unsuccessful authentication attempts using the same userID. The locking mechanism must be reversible by an administrator and should be reversible after a configurable time period.

CHANGE - Requirement: R-78010 (VNFRQTS-838)
The VNF **MUST** integrate with standard identity and access management protocols such as LDAP, TACACS+, Windows Integrated Authentication (Kerberos), SAML federation, or OAuth 2.0.

- Identify protocols to support
- "OAuth 2.0 with an operator provided Authorization Server"
- 2/11 Need feedback from Vendors

The VNF **MUST** support LDAP in order to integrate with an external identity and access manage system. It **MAY** support other identity and access management protocols.

REMOVE - Requirement: R-85419 (VNFRQTS-839)
The VNF **SHOULD** support OAuth 2.0 authorization using an external Authorization Server.

- 2/11 should be combined, dependent on feedback from vendors on R-78010

CHANGE - Requirement: R-581188 (VNFRQTS-825)
A failed authentication attempt **MUST NOT** identify the reason for the failure to the user, only that the authentication failed.

The VNF **MUST NOT** identify the reason for a failed authentication, only that the authentication failed.

CHANGE - Requirement: R-479386 (VNFRQTS-840)
The VNF **MUST NOT** display “Welcome” notices or messages that could be misinterpreted as extending an invitation to unauthorized users.

The VNF **MUST** provide the capability of setting a configurable message to be displayed after successful login. It **MAY** provide a list of supported character sets.

- Ask Trevor Lovett if the supported character sets are specified in the VNF requirements
    - Answer (23/2/2020): Not to his knowledge.

CHANGE - Requirement: R-231402 (VNFRQTS-826)
The VNF **MUST** provide a means for the user to explicitly logout, thus ending that session for that authenticated user.

The VNF **MUST** provide a means to explicitly logout, thus ending that session.

NEW REQUIREMENT (VNFRQTS-827)

The VNF **MUST** provide explicit confirmation of a session termination such as a message, new page, or rerouting to a login page.

CHANGE - Requirement: R-45719 (VNFRQTS-828)
The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, or enforce a configurable “terminate idle sessions” policy by terminating the session after a configurable period of inactivity.

The VNF **MUST**, if not integrated with the Operator’s Identity and Access Management system, enforce a configurable “terminate idle sessions” policy by terminating the session after a configurable period of inactivity.

El Alto

CIS_Docker_Benc...mark_v1.2.0.pdf

Casablanca

Please provide comments through the JIRA tickets.

2018-09-12_New...rementsV2.pptx