Organisation des tests de PRA

Architecture solution de PRA · https://preview.nuabee.fr/documents/organisation-tests-pra/

Principes des tests de PRA

Les tests de PRA couvrent deux aspects complémentaires :

- Le **test de secours informatique** qui a pour objectif principal de
  - Vérifier le bon fonctionnement des serveurs et Appliances en périmètre PRA
  - Vérifier la gestion des dépendances entre serveurs
  - Vérifier la connectivité WAN et le paramétrage du boitier en cas d'utilisation du boitier RCA

=> Ce test n'implique généralement pas de coupure de production.

- Le **test de reconnexion** qui a pour objectif principal de :
  - Vérifier la bascule du réseau de production
  - Tester la reconnexion mobilité (VPN SSL, ...)

=> Ce test implique une coupure de production de par sa nature.

Tests de secours informatique

Le test de secours informatique est, par défaut, semestriel et sa date définie entre les parties. Il se déroule en heures ouvrées et consiste à redémarrer dans l'espace de secours du client dans le cloud:

- L'ensemble des serveurs du périmètre du PRA,
- Les éventuelles appliances de sécurité du périmètre du PRA,
- En cas d'utilisation du boitier RCA, le VPN de reconnexion du (des) site(s) utilisateur(s) au site de secours dans le cloud.

Le test de secours informatique porte sur :

- Les automatismes et les procédures de restaurations et de redémarrage,

- La vérification de la gestion des dépendances entre serveurs,
- Le bon fonctionnement des réseaux LAN et des serveurs redémarrés.

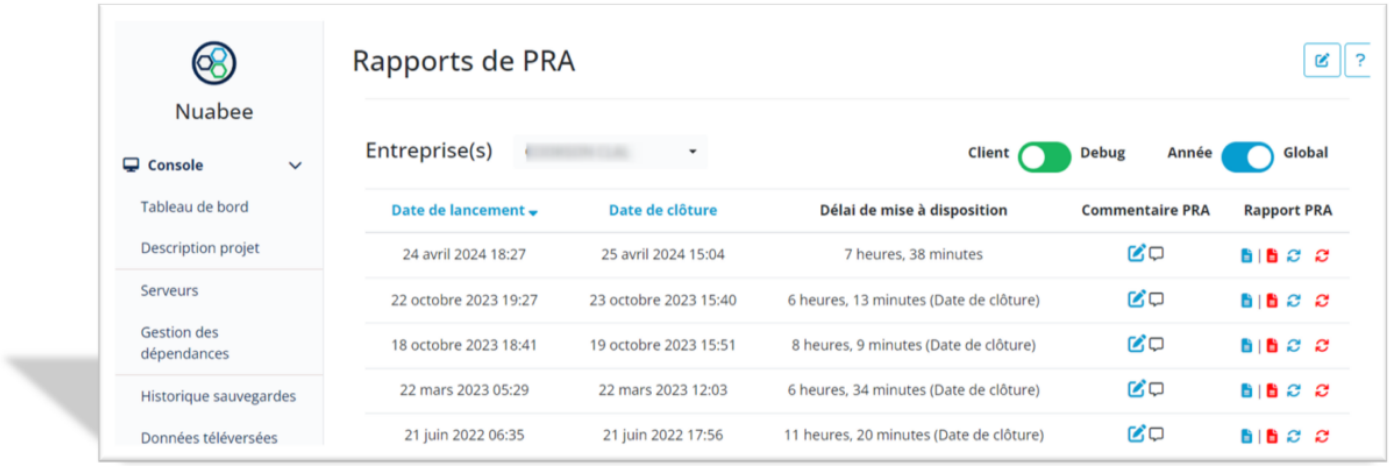
Le client a la responsabilité de faire le test sur chaque serveur et chaque application et d'indiquer ses tests dans la page de test de la Console Atlas.

Ce test est aussi l'occasion de constater d'éventuelles variations du périmètre du PRA et d'étudier s'il convient d'effectuer la modification des procédures associées.

Rapport de test de secours informatique

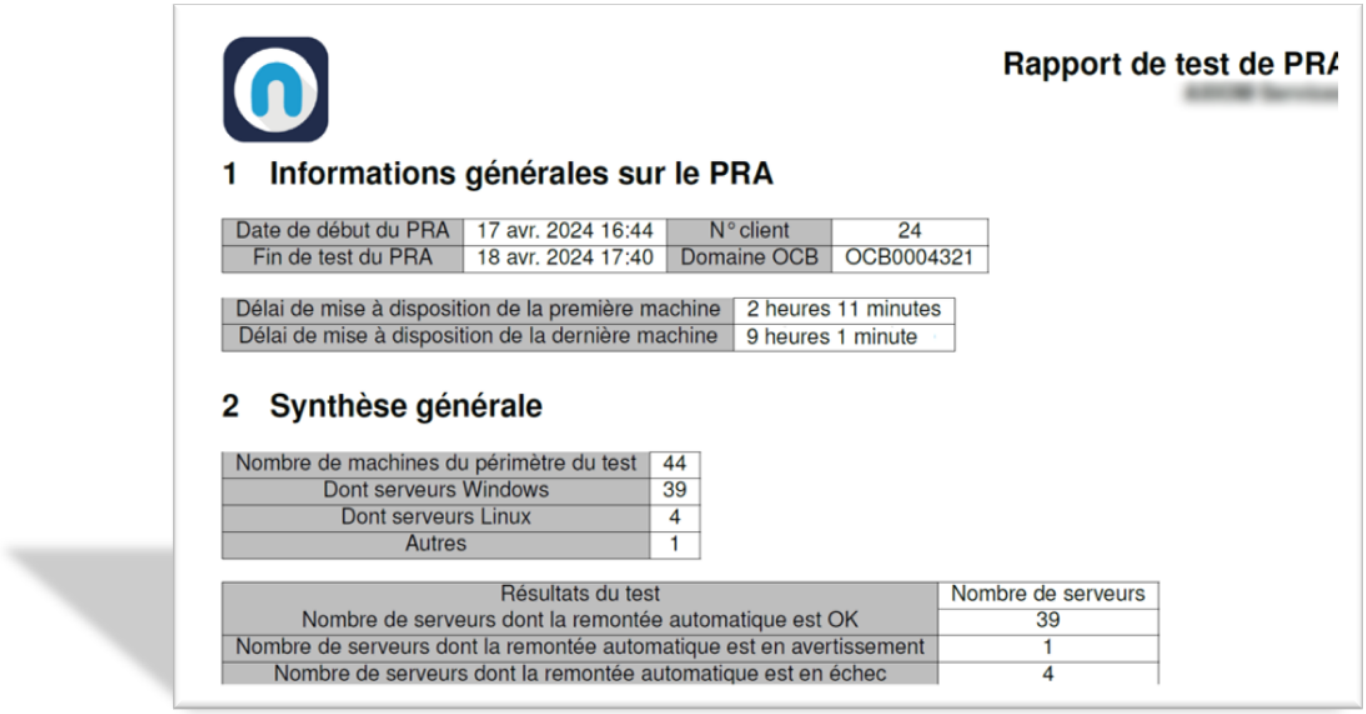
À chaque test, un rapport de test est généré et est stocké dans la Console Atlas.

Il intègre les commentaires des tests Client sur chaque serveur/application.



Ce rapport de test de PRA (document PDF) indique :

- Le délai de mise à disposition du premier serveur.
- Le délai de mise à disposition du dernier serveur.
- La synthèse générale.
- Puis, sur les pages suivantes, le détail du tests utilisateur pour chaque serveur/application.



Rapport de test de PRA

1 Informations générales sur le PRA

Date de début du PRA	17 avr. 2024 16:44	N° client	24
Fin de test du PRA	18 avr. 2024 17:40	Domaine OCB	OCB0004321

Délai de mise à disposition de la première machine	2 heures 11 minutes
Délai de mise à disposition de la dernière machine	9 heures 1 minute

2 Synthèse générale

Nombre de machines du périmètre du test	44
Dont serveurs Windows	39
Dont serveurs Linux	4
Autres	1

Résultats du test	Nombre de serveurs
Nombre de serveurs dont la remontée automatique est OK	39
Nombre de serveurs dont la remontée automatique est en avertissement	1
Nombre de serveurs dont la remontée automatique est en échec	4

À la suite de chaque test de secours informatique, il est défini dans ce rapport les éventuelles actions à mener.

Tests de reconnexion

La fréquence du test de reconnexion est dépendant de l'architecture du Client et est une extension demandée par le Client lors de la planification d'un test de secours informatique standard. Ce type de test demande une organisation au niveau Client car cela signifie coupure de la production. Il est effectué en heures non-ouvrées.

Il consiste à vérifier la bascule du réseau de production du Client en cas d'activation d'un PRA et, suivant le périmètre du projet, de tester les mécanismes de reconnexion en mobilité (VPN SSL, ...).

Il se déroule en heures ouvrées et si l'architecture du client impose un test en heures non ouvrées, ceci donnera lieu à un devis complémentaire.

Un rapport est rempli par le client à la fin de se test afin d'en noter tous les aspects (ce qui a fonctionné ou non).

Dossier de reconnexion

Pour chaque client, un dossier de reconnexion est constitué.

Il comprend les éléments suivants :

- Les scénarios de risques à couvrir
- Le schéma d’architecture réseau
- Les opérations sur le réseau à réaliser avant ou après bascule en mode secours du côté client et du côté Nuabee