Processus de qualification d’un projet PRA

Architecture solution de PRA · https://nuabee.fr/documents/processus-qualification-projet-pra/

Principaux objectifs du processus de qualification

Lors des premiers échanges sur un projet de PRA, l’un des axes abordés consiste à qualifier le périmètre du projet, l’architecture réseau et les contraintes de sécurité.

- Définition des scénarios à couvrir

Comme explicité dans la KB « Comment établie un PRA efficace » , le premier point à aborder concerne les scénarios de risques à couvrir. La qualification dépendant du ou des scénarios à prendre en compte, il est important de le définir dès le départ du projet, les choix de périmètre et de reconnexion peuvent en découler.

- Définitions du périmètre serveur à couvrir

Quand les scénarios de risques à couvrir sont arbitrés, il faut définir le périmètre serveur à couvrir. En effet, le but d’un PRA est de permettre de redémarrer afin de limiter les pertes liées à un interruption d’activité. Il faut alors identifier quels sont les serveurs et autres appliances sans lesquelles l’entreprise ne peut fonctionner.

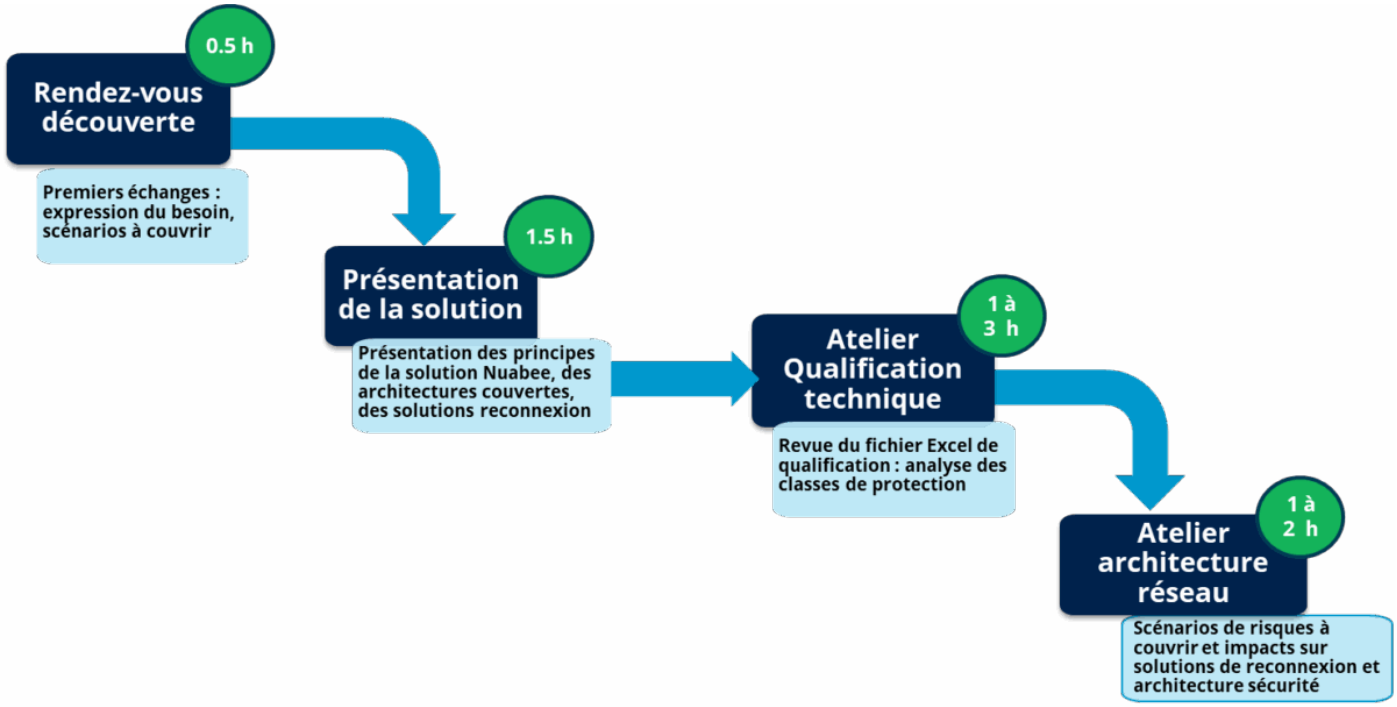
Une fois chose faite, Nuabee proposant des classes de protection il est alors possible de classer en trois niveaux de criticités les machines du parc:

- **La classe PRA**: Les machines identifiées comme faisait parti du cœur de métier et sans lesquels il serait impossible de fonctionner (Exemple: AD principal, serveur de fichier, ERP, BDD, serveur applicatif des machines de production, …).
- **La classe de sauvegarde avec tests**: Les machines qui ne sont pas indispensable au fonctionnement et ne nécessitant pas de RTO garanti mais pouvant s’avérer utiles dans un second temps ou en cas de défaillances (Exemple: AD secondaire, serveur d’impression, serveurs d’applications peu utilisées, etc…)
- **La classe de sauvegarde sans test**: Le reste du parc qui aurait besoin de sauvegarder externalisé afin de ne pas repartir de zéro en cas de destruction totale du site ou de ransomware (Exemple: Archives, Serveurs de tests, Serveur VCSA, etc…) .

- Définition du périmètre réseau: interconnexions pour la reconnexion des sites et des utilisateurs

L'un des axes important du PRA, sans lequel ce ne serait que des backups externalisés, concerne les moyens de reconnexion en cas de bascule qui, comme pour les sauvegardes (quelque soit la classe de protection), doivent être définis et testés. Ainsi il faut qualifier les différentes connexions entre les différents sites clients ou encore les utilisateurs en mobilité.

Les étapes et ateliers de qualification



Etape	Objectifs	Durée estimée	Livrable
1 – Rendez-vous découverte	Premiers échanges : expression besoin de cyber-résilience, scénarios à couvrir	1h	Adéquation solutions Nuabee
2 – Présentation de la solution	Présentation des principes de la solution Nuabee, des architectures couvertes, des solutions reconnexion, des classes de protection	Environ 1h30	Document de synthèse de la solution.

3 – Atelier qualification technique	Echange sur le périmètre du projet en général. Validation du périmètre des serveurs et des rôles des serveurs.	Suivant périmètre projet (de 1 à 3 h)	Fichier Excel à remplir avec toutes les informations sur les serveurs énoncés lors des différentes échanges et demandant d'autres informations permettant d'établir une proposition technique et commerciale sera envoyé.
4 – Atelier architecture réseau	Le but principal de cet atelier est de bien redéfinir les scénarios de risques à couvrir et ainsi de proposer une solution de reconnexion. Cet atelier peut mener à d'autres ateliers si, par exemple, le prestataire du client gérant le réseau WAN du client (MPLS, SASE, etc…) doit intervenir pour prévoir la mise en place de nouvelles interconnexions, routes, etc… lors de la mise en place du PRA.	Suivant périmètre projet et architecture réseau : un ou plusieurs ateliers d'1h30	A la fin de ces atelier, un document récapitulatif (PPT) des propositions de reconnexion sera fourni afin d'avoir une base lors de la phase d'Onboarding.