DRP project qualification process

DRP solution architecture · https://nuabee.com/documents/qualification-process-drp-project/

Main objectives of the qualification process

During the initial discussions on a DRP project, one of the main objectives is to qualify the project scope, network architecture and security constraints.

- Defining the scenarios to be covered

As explained in KB "How to set up an effective DRP", the first point to address concerns the risk scenarios to be covered. As qualification depends on the scenario(s) to be taken into account, it is important to define it at the outset of the project, as the choices of perimeter and reconnection may result from it.

- Defining the server perimeter to be covered

Once the risk scenarios to be covered have been determined, it's time to define the server perimeter to be covered. Indeed, the aim of a DRP is to enable restarting in order to limit losses linked to a business interruption. It is therefore necessary to identify the servers and other appliances without which the company cannot function.

Once this has been done, as Nuabee offers protection classes, it is then possible to classify the machines in the park into three levels of criticality:

  - **PRA class**: machines identified as being part of the core business, and without which it would be impossible to operate (e.g. main AD, file server, ERP, DB, application server for production machines, etc.).
  - **Backup class with tests**: Machines which are not essential to the operation and do not require a guaranteed RTO, but which may prove useful at a later date or in the event of failure (e.g. secondary AD, print server, little-used application servers, etc.).
  - **The non-test backup class**: The rest of the park that would need to be backed up externally, so as not to start from scratch in the event of total site destruction or ransomware (e.g. Archives, test servers, VCSA server, etc.).

- Defining the network perimeter: interconnections for reconnecting sites and users

One of the most important aspects of the DRP, without which it would be no more than outsourced backups, concerns the means of reconnection in the event of a switchover. As with backups (whatever the protection class), these must be defined and tested. This means qualifying the various connections between different customer sites or mobile users.

Stages and workshops

Stage	Objectives	Estimated duration	Deliverable
1 - Discovery meeting	First discussions: expression of needs, scenarios to be covered	1h	Matching Nuabee solutions
2 - Solution overview	Presentation of Nuabee solution principles, architectures covered, reconnection solutions	Approx. 1h30	Solution summary document.
3 - Technical pre-qualification	Exchange on the general scope of the project	Depending on project scope	An Excel file to be filled in with all the information on the servers listed during the various exchanges and requesting other information enabling a technical and commercial proposal to be drawn up will be sent.

4 - Network workshop	The aim of this workshop is to redefine the scenarios to be covered and thus propose a reconnection solution. It often enables us to correct misunderstandings about the current network, and allows us to foresee several study cases to be validated. It also provides an opportunity to revisit any network aspects that may not have been addressed or forgotten during the first Nuabee-Customer exchange. This workshop can lead to other workshops if, for example, the customer's service provider managing the customer's WAN network (MPLS, SASE, etc.) needs to intervene to plan the implementation of new interconnections, routes, etc. during the implementation of the DRP.	Depending on project scope and network architecture: 1 or more 1h30 workshops	At the end of these workshops, a summary document (PPT) of the reconnection proposals will be provided as a basis for the Onboarding phase.