



FORMATION : INFRASTRUCTURE SYSTÈME

DI-131b: Administration DNS avancée et sécurité (3 jours)

Logiciels utilisés

ISC **Bind Server** sur système GNU/Linux

Présentation

Bind est l'implémentation du protocole DNS le plus répandu. Ce protocole est désormais indissociable des réseaux IP et des services associés. Développé par l'Internet Software Consortium (ISC), Bind équipe la majorité des serveurs DNS publics. Ce module permet d'acquérir les connaissances nécessaires au déploiement et à l'administration de tels serveurs DNS, qu'il soit à usage interne ou externe.

Cette formation complète la formation DI-131 (Déployer un serveur DNS) en traitant de la messagerie, de la sécurité, du partage de charge, ...

Objectifs

Ce stage permet la découverte de l'implémentation libre du protocole DNS au travers du serveur Bind. Après une présentation de l'architecture DNS et son implication dans les réseaux IP, les stagiaires réaliseront une maquette complète d'une telle architecture. Les mécanismes plus poussés offerts par Bind seront également abordés : mise à jour automatique, chiffrement, délégation, partage de charge, messagerie, sécurité avancée, ...

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des réseaux TCP/IP

Programme

<p>JOUR 1</p> <p>DNS et la messagerie</p> <ul style="list-style-type: none"> ● Les pointeurs MX ● Les enregistrements inverses (PTR) ● DNS et les protections Antispam ● DNS et les blacklists (RBL) ● Le "Sender Policy Framework" (SPF) et « sender-id » <p>Sécurisation d'une installation DNS</p> <ul style="list-style-type: none"> ● Connaître les principales failles et erreurs de configuration ● Étude de la faille de Juillet 2008 ● Tester la sécurité d'un serveur ● Récursivité, transfert de zone ● Utilisation des « vues » 	<p>JOUR 2</p> <p>Maquette générale :</p> <p>Utilisation de DNSSEC</p> <ul style="list-style-type: none"> ● Présentation du mécanisme ● Impacts sur la sécurité du protocole DNS ● Mise en oeuvre avec Bind <p>Sécurisation d'une installation DNS</p> <ul style="list-style-type: none"> ● Redondance ● Sécurisation ● Tests <p>JOUR 3</p> <p>Load-balancing avec DNS</p> <ul style="list-style-type: none"> ● Partage de charge entre serveurs DNS ● DNS pour répartir la charge entre serveurs HTTP ● Les enregistrements SRV <p>Multicast DNS</p> <ul style="list-style-type: none"> ● Présentation du mécanisme ● Implémentations Avahi, Bonjour et Zeroconf ● Active Directory et DNS <p>Maquette</p>
--	--

Le programme ci-dessus présente le programme initial de la formation DI-131b d'une durée de 3 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin. Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.