Pearson

Q-Interactive

Exigences du réseau pour Q-interactive Assess

Aperçu

Ce guide vous aidera à vous assurer que votre environnement réseau est optimisé afin que l'application Q-interactive Assess puisse partager des renseignements entre les appareils du client et du praticien. Bien qu'Assess ne nécessite pas de connexion Wi-Fi active, les protocoles de communication du réseau doivent être corrects et activés pour que les appareils se découvrent automatiquement les uns les autres au moyen de la technologie Bonjour d'Apple. Le présent document donne un aperçu des exigences du réseau nécessaires au bon fonctionnement de Bonjour.

Pour plus d'information sur Bonjour, consultez la documentation d'assistance d'Apple.

Réseau local

Assess utilise une méthode de connexion directe pour communiquer à travers le réseau local. Dans les environnements comportant plusieurs nœuds sans fil, la communication de nœud à nœud doit être activée. Vos appareils doivent se trouver sur le même réseau VLAN ou sous-réseau au sein du réseau pour se connecter. La technologie Bonjour d'Apple ne peut pas traverser les sous-réseaux/réseaux VLAN de façon native. Si vos appareils doivent se trouver sur des sous-réseaux différents, une passerelle Bonjour peut être nécessaire pour votre réseau. Bien que certains matériels réseau intègrent cette fonctionnalité, d'autres peuvent nécessiter une solution tierce. Une passerelle Bonjour permet à Bonjour de traverser les sous-réseaux/réseaux VLAN afin que vos appareils puissent communiquer. Aerohive et Cisco sont deux développeurs de passerelles Bonjour.

Multidiffusion

Votre réseau local doit être autorisé à exécuter Bonjour et mDNS (DNS multidiffusion).
La multidiffusion doit également être activée, mais l'abandon de la multidiffusion doit être désactivé.

Le protocole Bonjour se compose d'annonces et de requêtes de services qui permettent aux appareils de demander et de promouvoir des applications spécifiques. Le DNS-SD (système de noms de domaine – découverte des services) sur un lien de multidiffusion est utilisé pour interroger le réseau local sur les services enregistrés. Chaque requête ou annonce est envoyée à l'adresse de multidiffusion Bonjour pour être distribuée à tous les clients du sous-réseau.

Le protocole Bonjour d'Apple repose sur le fonctionnement du mDNS à partir du port UDP 5353

et effectue des envois à ces adresses de groupe réservées :

- Adresse de groupe IPv4 - 224.0.0.251
- Adresse de groupe IPv6 - FF02::FB

Les adresses utilisées par le protocole Bonjour sont des adresses multidestinataires link-local et ne sont donc transmises que localement. *Les routeurs ne peuvent pas utiliser le routage de multidiffusion pour rediriger le trafic, car la durée de vie est fixée à un, et la multidiffusion link-local est censée rester locale.*

Pour obtenir la liste complète des ports TCP et UDP utilisés par les logiciels Apple, consultez la documentation d'assistance d'Apple.

Groupes de multidiffusion

Certains réseaux peuvent utiliser un groupe de multidiffusion pour gérer le trafic de multidiffusion. Lorsque la multidiffusion est activée, tout le trafic de multidiffusion est acheminé vers tous les clients connectés d'un sous-réseau. En utilisant un groupe de multidiffusion pour limiter le nombre de clients recevant les données de multidiffusion, vous pouvez réduire la charge de travail globale étant placée sur le réseau.

L'utilisation de groupes n'est généralement pas nécessaire, mais elle peut s'avérer utile s'il y a de nombreux appareils Bonjour sur le réseau.

Lors de la création de groupes de multidiffusion, trois facteurs importants doivent être pris en compte :

1. Les groupes de multidiffusion doivent inclure les sous-réseaux ou les réseaux VLAN où les appareils Assess sont connectés.
2. Tous les appareils Assess doivent être membres du groupe de multidiffusion.
3. Si vous utilisez des groupes de multidiffusion, la surveillance de trafic du IGMP doit être activée sur votre réseau pour permettre à vos appareils d'écouter le groupe de multidiffusion. Cela permet à vos appareils de voir le trafic du groupe de multidiffusion sans avoir d'incidences sur le reste de votre réseau.

Sécurité du protocole Bonjour

Afin d'atténuer les risques associés au protocole Bonjour d'Apple, Q-interactive utilise un code de déverrouillage interne secret pour établir une connexion sécurisée entre les appareils. Pour améliorer encore davantage la sécurité, les administrateurs réseau peuvent choisir de mettre en œuvre une segmentation, des contrôles d'accès et/ou un filtrage du trafic afin de limiter l'utilisation de Bonjour aux seuls services nécessaires.

Pour sécuriser un réseau afin de n'autoriser que le service spécifique pour Q-interactive tout en bloquant les autres, suivez ces étapes générales :

1. Identifier le service Bonjour requis
   - Chaque service Bonjour dispose d'un type de service unique. Le nom du service de Q-interactive est _assess2._tcp.
2. Mettre en place les réseaux VLAN et la segmentation
   - Créez un réseau VLAN distinct pour les appareils qui doivent utiliser le service Bonjour.
   - Utilisez une passerelle Bonjour ou un répéteur mDNS (si nécessaire) pour permettre la découverte des services entre les réseaux VLAN tout en bloquant les autres services.
3. Contrôler le trafic mDNS à l'aide de règles de pare-feu
   - Autorisez uniquement le trafic mDNS (port UDP 5353) pour le service spécifique et bloquez les autres.

- Exemple de règle :
  - Autoriser le trafic UDP 5353 pour _assess2._tcp
  - Refuser tout autre trafic mDNS

4 Utiliser les listes de contrôle d'accès (LCA)

- Configurez les LCA afin que seuls les appareils qui ont besoin du service puissent envoyer ou recevoir des paquets mDNS pour ce service.
- Exemple de LCA (sur un commutateur ou un routeur géré) :
  - **Autoriser** le trafic mDNS pour _assess2._tcp
  - **Refuser** toute autre diffusion mDNS

5 Configurer les commandes de découverte de réseau

- Si votre équipement de réseau prend en charge la fonction de surveillance de trafic mDNS, activez cette fonction afin de filtrer le trafic indésirable de Bonjour.

  Désactivez les services Bonjour/mDNS sur les appareils qui n'en ont pas besoin afin de réduire l'encombrement du réseau.

6 Utiliser la gestion des appareils mobiles (GAM) ou les contrôles au point terminal

- Utilisez les politiques de GAM pour n'autoriser que le service Bonjour requis sur les appareils.
- Limitez les activités indésirables de Bonjour telles que AirPlay, le partage de fichiers ou d'autres services Bonjour à l'aide des profils de configuration des appareils.

7 Surveiller et enregistrer le trafic mDNS

- Utilisez des outils de surveillance du réseau pour vérifier que seul le service autorisé est annoncé.
- Configurez des alertes pour les services Bonjour non autorisés apparaissant sur le réseau.

En isolant, filtrant et/ou restreignant le trafic Bonjour, vous pouvez sécuriser votre réseau tout en autorisant les services souhaités, tels que Q-interactive.

En utilisant tous les renseignements contenus dans ce guide, vous devriez être en mesure de vous assurer que tout réseau est configuré de manière optimale pour Q-interactive Assess.

Pour obtenir des réponses à des questions spécifiques ou des détails de configuration plus avancés, communiquez avec le fabricant de votre matériel réseau.

Communiquez avec nous au 1 866 335-8427

Pour en savoir plus : PearsonClinical.ca