Que faire lors de l'erreur "Action manuelle requise - Vérifiez la connectivité réseau" sur le déploiement de MAV ?

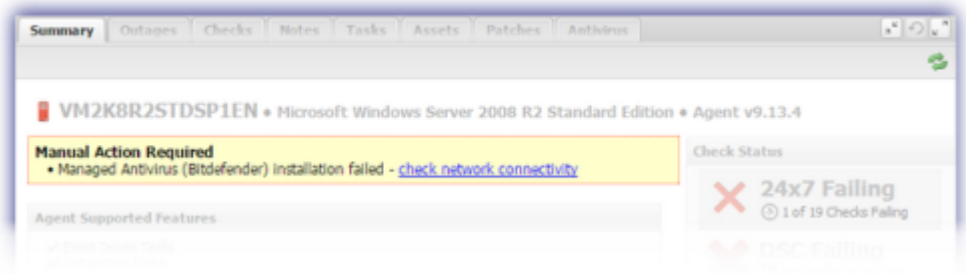
Guillaume - 2020-06-17 - N-sight RMM

Action manuelle requise - Vérifiez la connectivité réseau

Lorsque le déploiement de Managed Antivirus (Bitdefender) échoue sans renvoyer un code d'erreur, l' onglet **Résumé** du périphérique affiche l' **action manuelle requise - L'installation de Managed Antivirus (Bitdefender) a échoué - vérifiez le** message d'erreur de **connectivité réseau** .

Cette condition d'erreur est généralement causée par l'échec du téléchargement du programme d'installation de Managed Antivirus (Bitdefender) et peut résulter d'un problème de connectivité entre l'appareil et le serveur de téléchargement.

Pour aider à résoudre les problèmes de communication potentiels, à partir du tableau de bord 6.17.2, nous avons inclus une tâche automatisée antivirus géré - connectivité réseau . Cela peut être déployé sur les appareils rencontrant actuellement ce problème ou sur les appareils avant l'installation de Managed Antivirus (Bitdefender) pour vérifier que les URL du serveur de téléchargement sont accessibles à partir de l'appareil.



Ajouter la Tache Automatisée

Pour ajouter la tâche automatisée **Antivirus géré - Connexion réseau à** partir du tableau de bord à un appareil:

1. Sur le Dashboard, sélectionnez l'appareil concerné
2. Dans l'onglet tache, sélectionnez Ajouter une tache automatisée
3. Recherchez la tâche
4. **Cliquez** sur **Ajouter** pour ouvrir l'assistant de configuration. Utilisez **Suivant** et **Précédent** pour la navigation
    1. Choisissez **Antivirus géré - Connexion réseau** de **Sélectionnez Script**
    2. Entrez un **nom descriptif** pour identifier la tâche sur le tableau de bord et

dans les rapports

3. Dans le menu déroulant **Sélectionnez la fréquence de la méthode,** définissez la planification sur **Manuel** car il s'agit d'une tâche à exécuter une seule fois pour vérifier la connectivité
4. Configurer la durée des tâches et le comportement d'exécution

Exécutez la tâche automatisée à partir du tableau de bord
Une fois la tâche automatisée téléchargée et synchronisée avec le tableau de bord, elle peut maintenant être exécutée:

Cliquez sur le poste en question, dans l'onglet **Tâches**, faites clique droit sur la tâche correspondante, **Exécuter une tache automatisée**

Onglet Tâches (appareil unique)

1. Mettez en surbrillance l'ordinateur dans le volet nord
2. Accédez à son onglet **Tâches**
3. Le résultat est affiché dans la colonne **Sortie** pour **Antivirus géré - Connectivité réseau**
4. Cliquez sur le lien **Sortie** pour **plus d'informations**

Production	Remarques
OK	La tâche automatisée a correctement interrogé les URL du serveur de téléchargement
Inaccessible	La tâche automatisée n'a pas pu interroger l'URL du serveur de téléchargement

URL de liste blanche
Lorsque des problèmes de connectivité sont signalés entre l'appareil et nos serveurs, nous suggérons de mettre en liste blanche les URL de gestion antivirus et de définition suivantes dans le pare-feu ou le logiciel de surveillance Web, puis vérifiez qu'elles sont accessibles à partir de l'appareil:

	URL de communication	
Territoire du tableau de bord	**URL**	**Emplacement du serveur**
Asie, Australie	ap-southeast-2.breckenridge.remote.management breck-ap-southeast-2-svc.logicnow.us cannonball-ap-southeast-2-push.logicnow.us	Australie
Europe, France (.fr), France1, Irlande, Pologne, Royaume-Uni	eu-west-1.breckenridge.remote.management	Irlande

	URL de communication	
	breck-eu-west-1-svc.logicnow.us	
	cannonball-eu-west-1-push.logicnow.us	
Allemagne	eu-central-1.breckenridge.remote.management	Allemagne
	breck-eu-central-1-svc.logicnow.us	
	cannonball-eu-central-1-push.logicnow.us	
Amériques, États-Unis	us-west-2.breckenridge.remote.management	États Unis
	breck-us-west-2-svc.logicnow.us	
	cannonball-us-west-2-push.logicnow.us	

Bitdefender Engine - Serveurs de mise à jour de fichiers et de définitions

breck-update.logicnow.us

breck-files.logicnow.us

data.cdn-sw.net

Pour simplifier la configuration du pare-feu et minimiser l'impact des modifications futures des URL, nous vous suggérons de mettre en liste blanche les domaines suivants:

Domaines de liste blanche (recommandé)

Pour simplifier la configuration du pare-feu et minimiser l'impact des modifications futures des URL, nous vous suggérons de mettre en liste blanche les domaines suivants:
* .remote.management
* .logicnow.us
* .cdn-sw.net
* .bitdefender.net
* .bitdefender.com
* .v1.bdnsrt.org