Comment fonctionne le VSS de N-able EDR ?

Stéphane Hoarau - 2021-03-19 - N-able EDR

L'agent SentinelOne prendra (par défaut) un instantané du système (peu importe l'utilisateur connecté, c'est pour l'ensemble de la machine) à chaque redémarrage et toutes les 4 heures depuis le dernier redémarrage.

Ces instantanés sont ensuite créés via le vss writer propre à EDR afin de créer de nouvelles copies du système.

Pour tous les instantanés VSS créés par l'agent, ils seront listés lorsqu'ils seront visualisés localement sur la machine avec la commande vssadmin de Windows.

Ainsi, si vous utilisez vssadmin, vous pouvez lister toutes les copies réalisée et marqué avec Type : application Rollback sont celles créées par l'agent SentinelOne.
Elles sont toutes horodatées pour que vous sachiez à ce moment-là quand le dernier instantané a été créé.