Présentation OSSIR

UserLock

Comment sécuriser l'activité des logons/logoffs dans les environnements Windows ?

CoperNet

Microsoft CERTIFIED Partner

L’authentification NT

- Elle conditionne souvent l’accès à la messagerie, à la comptabilité, aux données commerciales… car la gestion de la sécurité est très souvent intégrée à Windows.

- Il est donc primordial que les utilisateurs utilisant un login soient bien les personnes auxquelles ils ont été attribués. Le cas contraire pourrait permettre l’accès à des données confidentielles.

Accès concomitants

- Windows ne permet pas d'interdire à un même compte utilisateur d'être connecté de façon interactive sur plus d'une machine en même temps.

- Dans le cas de réseaux avec des postes à libre accès, les utilisateurs oublient parfois de se déconnecter : ce qui rend alors accessible à n'importe qui les informations accessibles par ce compte. La création d'une politique limitant les logons concomitants contribue à améliorer la vigilance des utilisateurs.

- De plus, même si un utilisateur a le mot de passe d'autrui, il ne peut usurper son identité pour peu que l'utilisateur réel soit connecté.

Un suivi des logons

- UserLock permet d'être alerté (mail, popup) en temps réel pour des groupes ou des utilisateurs spécifiques en cas de:
  - Connexion réussie
  - Connexion échouée
  - Déconnexion
- Toute l'activité est journalisée
- UserLock présente un tableau de bord : "Qui est connecté où ?"

CoperNet

Microsoft CERTIFIED Partner

Intégration à Windows

- UserLock fonctionne comme service NT.
- Il déploie automatiquement et de façon transparente ses agents sur les stations à protéger.
- Chaque agent consiste en une GINA qui vient compléter le processus d'authentification natif de Windows.
- La GINA localise les serveurs UserLock à l'aide de DNS