Global Security Group Monitoring

Wednesday, November 26, 2014
2:21 PM

Theory

Monitors for users being added or removed from security groups. Monitoring is based parsing event logs.

Instructions

1. Copy the contents of the 'Install Security Group Monitors' file.
2. Paste the copied contents in to SQLyog.
3. Modify the values for the AlertID and GroupID if required.
   a. By default, it will install with Default - Create LT Ticket and Server Managed 24x7 group.

Itemize Inventory

1. LT Monitors - Installed on the Server Manage 24x7 Group (By Default)
   a. EV - User Added to Security Group - Schema Admins
   b. EV - User Added to Security Group - Administrators
   c. EV - User Added to Security Group - Domain Admins
   d. EV - User Added to Security Group - Enterprise Admins
   e. EV - User Remove from Security Group - Schema Admins
   f. EV - User Remove from Security Group - Administrators
   g. EV - User Remove from Security Group - Domain Admins
   h. EV - User Remove from Security Group - Enterprise Admins

Change Log

1. 2014-11-26 - Solution Finalized [BKO]

Authors

1. Original Creator
   a. Brian Ojeda - LabTech ServicePlus
2. Contributors
   a. N/A