Active directory domain

PARTNER UPDATE – January 21st, 2021

Dear KIS Clients,

An often-overlooked aspect of IT security is using an Active Directory domain administrator account to run tasks and services on servers. We frequently see this in the field, where an Administrator domain account (or their own admin-level account) was used to get a task or service up and running quickly and then forgotten.

When this happens, and the domain administrator account's password is changed (because you ARE changing that password on a regular basis, right?), suddenly a dozen different things seem to break...which means that you get to spend all of your time diagnosing what's broken and tracking down the service or task that's no longer running.

Server-oriented tasks and services should use either a local server account or a specific named domain account with sufficient security access to get the job done if domain authorization is required. Ideally, each service or task will have its own unique login and password.

If you're despairing of finding and correcting these services, we can help by surveying all of your domain-joined servers to see what accounts are being used to run server services and tasks, presenting you with a spreadsheet showing "who's running what where."

Armed with that spreadsheet, you (or we!) can then change each task or service to utilize a unique account so that changing your administrator password can be done without fear of breaking anything.

Thank you,

Allan

Allan Hurst
Partner, Director of Project Management Office
KIS - Keep IT Simple | Professional IT Solutions Experts Since 1988
E: hurst@kiscc.com
O: (510) 403-7500