Stanford | University IT
Information Security Office

Position Paper - Clarification on 2FA requirement for Linux server logins

Position Title	
Position Audience	Stanford Faculty, Staff, and Students
Contact	Information Security Office (https://stanford.service-now.com/it_services?id=sc_cat_item&sys_id=f7ae081a13bce2008a9175c36144b0ad)
Position Release Date	2023-06-23
Last Update	Initial Posting

Problem Statement

Per minimum security standards for moderate and high risk servers 2FA is required for user and administrator logins. However, there are some questions in regards to certain situations where it is hard to comply with this requirement. These include accounts used for automation and certain specific use-cases.

ISO Position

The reason for this requirement in MinSec is to prevent phished or otherwise compromised accounts being used for unauthorized access. So let's keep that in mind when we look at the applicability of this requirement.

Special cases: -

Automation: - Use dedicated service accounts with minimum required privileges for non-interactive automation processes. These accounts don't require 2FA. The 2FA requirement is meant to protect interactive logins by users or administrators.
Note: 2FA is required for interactive logins on a per-server basis. Logging in to a bastion host with 2FA does not eliminate the need for 2FA when connecting to other servers from that bastion host.

Compute clusters: - Dedicated compute clusters have a concept of virtual sessions spanning across multiple nodes. For example, a user can login to a login-node and launch a compute job which will run on one or more of the compute nodes. The user's login session allows them to check the status of the job on the compute node(s) where their job is running. This access is allowed only on the nodes where their jobs are running. 2FA is needed for users to login into the login-node. However, accessing compute nodes from the login node through this virtual login session doesn't need another 2FA verification..