Foreman - Feature #36650

Change Linux password hashing default from sha256 to sha512

08/07/2023 08:21 PM - Ewoud Kohl van Wijngaarden

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Unattended installations		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

https://wiki.archlinux.org/title/SHA_password_hashes states that NSA has recommended SHA512 since RHEL 5. This means it's safe to do with wide compatibility. It should be noted that Fedora 35 has started to default to YESCRYPT. See ENCRYPT_METHOD in /etc/login.defs and https://www.fedoraproject.org/wiki/Changes/yescrypt_as_default_hashing_method_for_shadow for more info.