SALTSTACK

SaltStack Enterprise 6.4.0

Release Notes

Document Last Updated*: October 2020*

What's in 6.4.0?

SaltStack® Enterprise 6.4.0 includes a variety of feature enhancements for SaltStack Comply and Protect and several customer-requested user interface improvements. This release also resolves several bugs and technical issues, especially for the LDAP and Active Directory authentication system.

Enhancements

General user interface improvements

This release includes several improvements to the overall functionality of SaltStack Enterprise user interface, including:

- Users can now run a command directly from a minion's detail page.
- The target create / edit dialog box now has an improved user interface that better manages how targets are defined when including operators.
- An improved unified component for dropdown inputs that allow for longer values.
- In cases where items have very long custom names (such as custom jobs or targets), those names are truncated in menus. The full name is displayed when hovering over the item with a mouse.
- Administrators can create custom warning or informational banners that can be displayed on the login screen for all users.
- Various input fields have been widened to allow for longer entries.
- Administrators can now create multiple types of Admin roles using the new Admin permission settings.

SaltStack Protect

This release included multiple improvements to SaltStack Protect:

- Users can view the status of the latest assessment and the latest remediation to determine whether it is queued, in progress, or complete from any page inside a Protect policy.
- While editing an assessment, users can select an option that will run the assessment immediately after saving.
- The user interface for editing policy names and defining targets on the same page has been streamlined and simplified.

SaltStack Comply

This release includes the following enhancements for SaltStack Comply:

- Custom variables for remediations now display a tooltip that informs users what the variable is and what values are expected and supported.
- Minions that are not applicable to a compliance result are no longer factored into compliance scores.
- While editing an assessment, users can select an option that will run the assessment immediately after saving.

LDAP and Active Directory

The 6.4.0 release of SaltStack includes several enhancements to the LDAP and Active Directory authentication system, including:

- Improved functionality in the user interface for selecting users contained inside nested groups or container groups.
- The prefill defaults are now more helpful and accurate.
- Improved search within the preview field.
- Improved support for OpenLDAP including configurable Group Name Attribute.

Related SaltStack Enterprise content releases

Some content published by SaltStack is released independently from the standard SaltStack Enterprise releases, including SaltStack Comply content and specialized Salt minion packages. Within this release cycle, the following new content and packages were made available:

- Ubuntu 16.04 CIS Benchmark for SaltStack Comply
- The DISA STIG RHEL7 Benchmark for SaltStack Comply

Issues resolved in this release

- In the user interface, compound targeting with grains does not work if the grain filter value contains spaces.
- If your File Server contains a large number of files, the File Server search functionality might lag.
- In some cases, SaltStack Comply and Protect assessments results might show a negative count of minions returned.

- In SaltStack Protect, vulnerability scans run immediately following a fresh installation of SaltStack Enterprise might fail. This happens because after the initial install, SaltStack Enterprise takes roughly 15-20 minutes to ingest vulnerability content.
- When importing a Tenable vulnerability scan through the Enterprise API (RaaS), the import may complete but will not change its status to complete on the backend and the user interface might stall while importing. This issue only occurs if the Tenable scan shows no vulnerabilities or if the Tenable scan does not cover any assets.
- When working with nested groups in LDAP, the Authentication workspace does not accurately reflect when a nested (or child) group is enabled. By enabling a parent group, you also enable all child groups by default. However, in the workspace, the child groups do not appear to be enabled.
- When configuring a Directory Service connection for a forest structure, the Auth Bind DN Filter field must be left blank.
- Any groups you have removed from an LDAP connection are still visible in the Roles workspace, and can be selected, although they are inactive. This also applies to any removed users previously visible in the Roles workspace. Although you can select an inactive group or user, these users can't log in to SaltStack Enterprise.
- SaltStack Enterprise might not correctly detect Active Directory members that belong to 20 or more groups.
- Active Directory users with Superuser access privileges may find their password settings are occasionally reset when they access the Authentication workspace (accessed from the Administration menu).

Feedback

Please submit any feedback using the form at https://saltstack.com/enterprisefeedback. You can also access the feedback form in SaltStack Enterprise by going to **Help > Feedback**.