

SALTSTACK®

SaltStack Enterprise 6.1.0

Release Notes

Document Last Updated: *October 2019*

What's in 6.1.0?

SaltStack Enterprise 6.1.0 includes the new SecOps Vulnerability Remediation add-on to bridge the gap between Security and IT teams. This add-on empowers either team to easily scan and remediate system vulnerabilities while still maintaining control over the entire process. This release also includes several crucial content updates, including a wide range of new SecOps Compliance content and the ability to create custom compliance content. Version 6.1.0 also includes improved credential and authentication management to ensure access to SaltStack Enterprise remains as secure as possible.

New features

SecOps Vulnerability

With the new SecOps Vulnerability add-on you can:

- View vulnerability assessment reports to identify a threat's severity level and help prioritize remediation efforts.
- Audit encrypted data records of all scans and remediations to identify who implemented changes and when.
- Export scan results as JSON records that can be imported to the third-party tools of your choice.
- Allow authorized users to add exemptions to exclude specific systems or vulnerabilities from remediation as needed.

This add-on currently supports RedHat, CentOS, Oracle Linux, SuSE, Ubuntu, Debian, and Amazon Linux. Additional operating systems will be supported soon.

SecOps Compliance content updates

This release includes an expanded live library with pre-built scans to detect and remediate thousands of critical vulnerabilities across a wide variety of systems. For example, version 6.1.0 now supports CIS for Debian Linux 9 Benchmark, CIS for Ubuntu 18.04 LTS Benchmark, and CIS Windows Server 2016 Benchmark.

SecOps Compliance custom content

Version 6.1.0 includes a Custom Content Software Development Kit (SDK) that can be used to create, test, and build custom security content. Import custom security content for use alongside SaltStack Enterprise's built-in security library for assessment and remediation.

Enhancements

Token authentication for Salt Masters

This release provides token authentication, a more secure method for authenticating and registering Salt Masters. A unique token is now auto-generated for each Salt Master that is registered within SaltStack Enterprise 6.1.0.

Encrypted credential management

Administrators now have the option to store PostgreSQL and Redis credentials in an encrypted file rather than the raas configuration file.

Directory service improvements

This release streamlines the process for connecting SaltStack Enterprise to an Active Directory (AD) or other Lightweight Directory Access Protocol (LDAP) server. Administrators can now preview users and groups before saving a Directory Service connection and can pre-populate common default settings for Active Directory, OpenLDAP, and other services. Administrators can also retrieve groups and users within a defined scope without synchronizing the entire directory.

Job descriptions

Users now have the option to add a description to jobs. This description will appear in the list of jobs in the Jobs workspace.

Issues resolved in this release

- Changing the LDAP or AD structure might prevent the SaltStack Enterprise LDAP/AD integration from pulling new users in from the directory. It might also prevent existing users from authenticating.
- `systemctl restart raas` may leave old SaltStack Enterprise processes running and prevent the newly started instance from functioning correctly.
- If the user who created one or more schedules is deleted, schedules created by that user will stop working.
- Rejected minion keys cannot be deleted. To delete a rejected minion key, first accept the rejected key and then delete it.
- Logrotate works only on files owned by root.
- When running jobs against a large number of minions, only the first 50 job returns show in SaltStack Enterprise console.

Feedback

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