TAM Service Engineer Engagement Check

OS and Certificate Assessment Report

for

Acme Corp

Prepared By: Adam Shambrook

Last Revision: v1.0.0

Last Revision Date: February 1, 2022

Document Summary

This Technical Account Management Service Engineer (TSE) quarterly engagement check report has been prepared after obtaining Puppet Server and Puppet Agent diagnostic and log information and focusing on Operating System and Certificate specific items. The Puppet TSE and Solution Architect teams have reviewed your specific environment details against Puppet Best Practices associated with Puppet Enterprise OS and Certificate deployment implementation.

This report will be presented during a customer advisory session to review the noted findings, suggested Puppet environment changes / updates and other Puppet recommendations. Optionally, your Puppet account team will follow-up with a SOW for a Puppet Professional Services Engineer or Puppet Solutions Architect to implement the recommendations if your team is unable to perform the suggested changes.

Engagement Check Contacts

	Puppet TAM	**Puppet TSE**	**Puppet Architect**
Name:	[Insert TAM Name]	[Insert TSE Name]	[Insert Architect Name]
Email:	[Insert TAM Email]	[Insert TSE Email]	[Insert Architect Email]

Engagement Check Summary

The Puppet Enterprise OS and Certificate assessment check will review your current Puppet Enterprise deployment implementation as follows:

1. Perform an analysis of your Puppet components against Puppet supported system requirements, including:
    a. Operating Systems
    b. Memory usage
    c. Hard drive capacity
    d. CPU usage
    e. Firewall configuration
2. Perform a Puppet certificate assessment to ensure no disruption between client and primary servers.

Recommendations

The following recommendations are suggested based on the performed OS and Certificate assessment check:

Recommended system requirements:

OS Check: Ubuntu 18.04 (amd64 architecture) with PE 2019.8.5.

- This is a supported OS for your current version of PE.

Memory Check: <10% used

- At the point in time of gathering this snapshot, your memory usage on your primary server has sufficient capacity.

Hard drive Capacity check: 60% Available (16GB+)

- While the primary server has sufficient storage capacity, your storage allocation appears to be all mounted on the root directory without segregating and assigning applications to use reserved portions. Puppet Enterprise's Code Directory and Postgres Database have the ability to grow. In your current configuration, one large file entering your code directory could fill the available storage space, impeding the Postgres DB which can lead to errors. Therefore, it is recommended that you define dedicated storage areas on your primary server to mitigate against this.

Firewall configuration:

- Complete. The firewall rules configured on the Primary Server OS host node enable Puppet to use the ports required by default.

Certificate verification and validity:

- Primary Server: The PE primary server's CA is valid for an additional 5 years. As such, this requires no action. The PE primary server's CA can be extended to 15 years if desired.
- General CA/Cert check: You have 80 nodes that have a CA expiring within 12 months, 10 of which within 3 months. These require you to renew the CA and Certs of these systems to prevent unnecessary disruption. Puppet recommends taking immediate action, minimally on the 10 servers nearing CA and cert expiration.

Puppet suggested planning recommendations:

a. While Ubuntu 18.04 is a supported operating system, the end of life is in April 2023 (14 months). Have you started planning for this event?
b. To improve your ability to view Postgres DB and the Code Directory capacity, consider reserving an allocated volume of storage for these resources.
c. Consider using the puppetlabs-ca_extend module from the forge to manage your certificate and CA expiry effectively. Details can be found here.

Other Noted Items:

d. You are currently using PE v.2019.8.5. While this is still supported, it is several versions behind LTS Puppet Enterprise version 2019.8.9. These updates include several feature enhancements currently unavailable to you, and CVE fixes that you remain vulnerable to. See the appendix below for a detailed list.
e. Your Primary server node seems to be running services other than the PE primary server. This is advised against, so services do not interfere with PE, and use resources that it expects should be available. Is it crucial to run these services on this node?

Appendix

PE release notes from v.2019.8.5 to v.2019.8.9.

Feature enhancements:

2019.8.6:

- Customize value report estimates
- Re-download CRL on a regular interval
- Remove staging directory status for memory, disk usage, and timeout error improvements
- Exclude events from usage endpoint response
- Return sensitive data from tasks
- Avoid spam during patching
- Parameter name updates
- Agent platform support for:
    - Fedora 32

2019.8.7:

- Update CRLs
- Filter by node state in jobs endpoint
- Sort activities by oldest to newest in events endpoint
- Export node data from task runs to CSV
- Disable force-sync mode
- Differentiate backup and restore logs
- Encrypt backups
- Clean up old PE versions with smarter defaults
- Agent platform support for:
    - macOS 11
    - Red Hat Enterprise Linux 8 ppc64le
    - Ubuntu 20.04 aarch64
    - Fedora 34

2019.8.8:

- Code Manager support for Forge authentication
- Puppet metrics collector module included in PE installation
- PE databases module included in PE installation
- Query by order and view timestamps in *GET /plan_jobs* endpoint
- Faster Code Manager deploys
- Client Tools platform support for:
    - macOS11

2019.8.9:

- TLS v1.3 is enabled by default
- Run patches sequentially in the group_patching plan
- Run the puppet infra run command with WinRM
- More options when running the support script
- Primary Server platform support for:
    - AlmaLinux x86_64 for Enterprise Linux 8
    - Rocky Linux x86_64 for Enterprise Linux 8

- Agent platform support for:
    - Ubuntu 18.04 aarch64
    - Debian 11 (Bullseye) amd64
    - Red Hat Enterprise Linux 8 FIPS x86_64
    - AlmaLinux x86_64 for Enterprise Linux 8
    - Rocky Linux x86_64 for Enterprise Linux 8

Common Vulnerabilities and Exposures fixed:

- CVE-2021-27026 - Sensitive Information May be Logged
- CVE-2021-27025 - Silent Configuration Failure
- CVE-2021-27023 - Unsafe HTTP Redirect
- CVE-2021-27022 - Information Disclosure in Logs
- CVE-2021-27021 - SQL Injection
- CVE-2021-27020 - Formula Injection
- CVE-2021-27019 - Verbose Logging

More information about these vulnerabilities can be found here