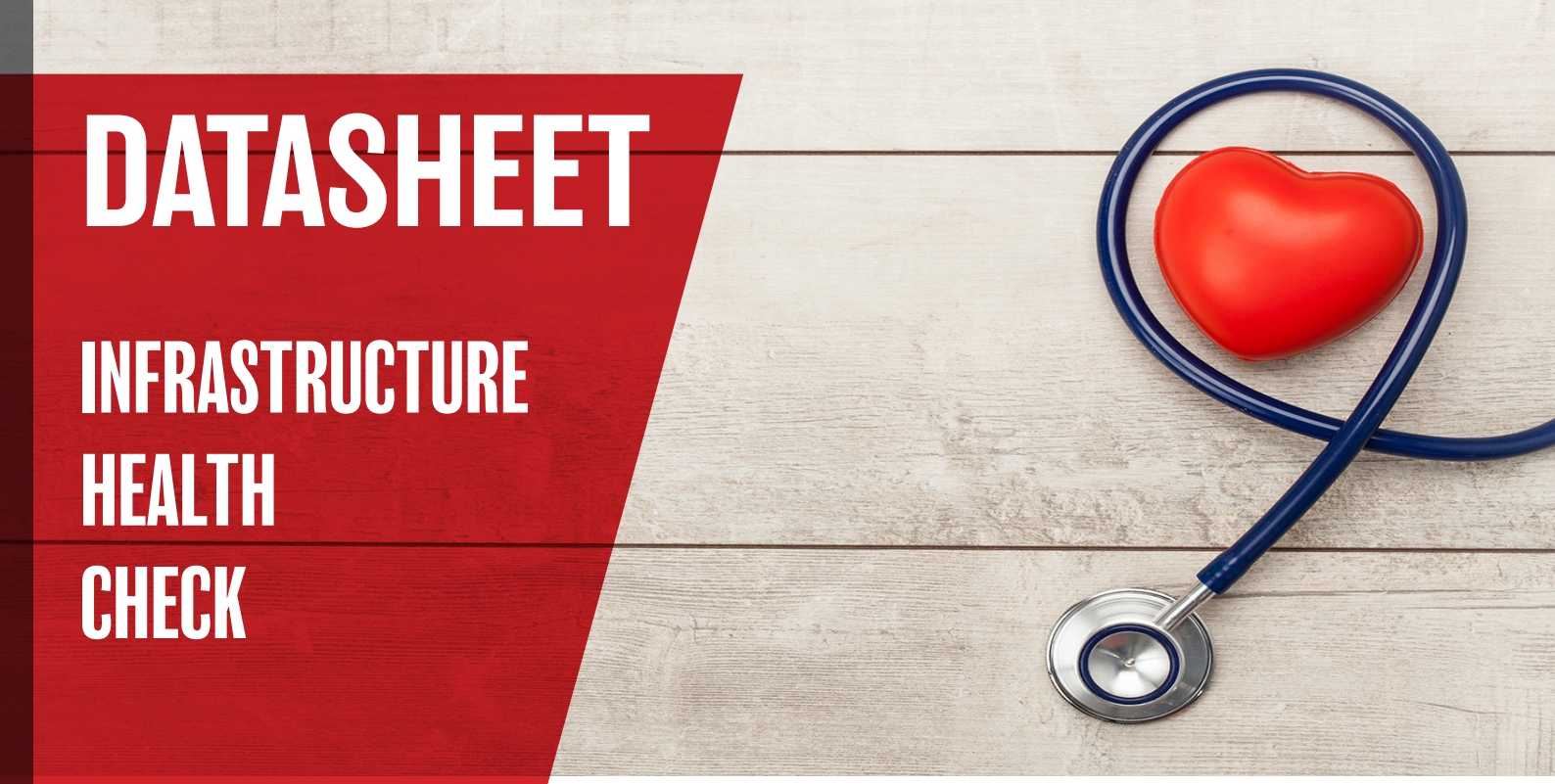
DATASHEET

INFRASTRUCTURE HEALTH CHECK



Proactive Oracle Infrastructure Health Checks

Claremont provides individualised health checks to their customers across multiple technology areas to ensure the in-place systems are not only fit for purpose but optimized to their most effective configuration. This allows customers to derive a greater return on investment from their IT systems and ensures they can concentrate on their core business function.

Claremont consultants are given the freedom to deliver. This means that when performing activities such as health checks they can use their skills, experience, and initiative to deliver a comprehensive health check tuned to the customer's requirements. This is done independently of any business development activities, ensuring there is no pressure on the consultant to deliver a health check that supports sales activities.

Claremont consultants are all senior consultants with 20+ years' experience, many have experience as users of the very applications that they now support. Our consultants have the expertise to perform an in-depth and thorough health check with a high degree of understanding as to the demands placed upon the customers IT systems.

Claremont's health check is typically performed by the Claremont consultant on-site at the customer offices, although it can in some instances be performed remotely. The Claremont consultant will discuss with the customer's IT team to understand at a high level the architecture and system configuration. It is expected that the customer IT team will be available throughout the health check to answer additional questions about environment specifics.

With an understanding of specific pain points and the environment's history, the consultant will run scripts to capture information from the customer system, and where relevant investigate specific areas of concern to uncover root causes. This captured information will then be reviewed, and initial findings shared with the customer before the consultant leaves the site.

Within a few days, the consultant will write up the findings, and report back to the customer the outcome of the health check. This will detail the checks performed, the issues found and, where relevant, corrective action recommended. It is then at the discretion of the customer whether those corrective actions are performed.

CLAREMONT

Support Status & Patching

A review of the versions of operating systems installed will be undertaken to verify this is in date with the software vendor. This ensures that should there be any issues with the software that support will be provided, and where applicable patches delivered.

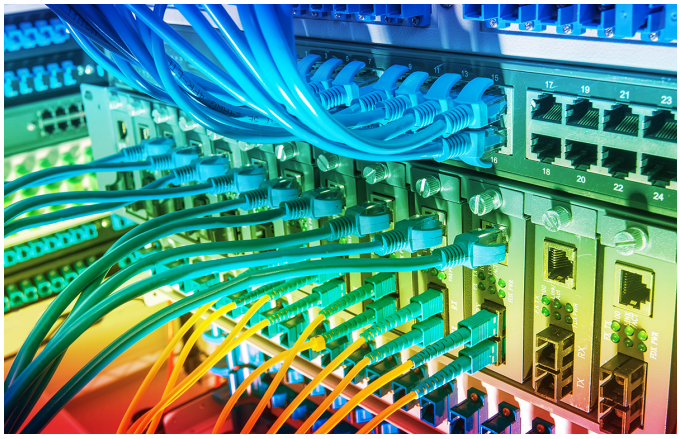
In some instances, there are valid reasons why support is allowed to lapse. Typically, due to legacy software support required for specific business functions. This will be recognized and noted by the consultant.

The consultant will also review the current state of patching on the system to ensure that regular and appropriate patching activity has taken place, to correct bugs discovered by the software vendor. The consultant will review the status of currently applied patches but will also review the process to apply patches with regards to change and version management and ensure that appropriate dispensation is made for testing prior to releasing patches into production.

General Architecture

A general architectural overview is essential to understanding the nature of the IT system. This will not be isolated to the system in question but will investigate the contact points with other periphery systems (for example, email, DNS etc.) which may have an operational impact on the smooth running of the system.

At a more technical level, the size and shape of the architecture will be reviewed, covering CPU configuration, memory configuration and disk configuration including RAID levels. Any clustering configuration will also be reviewed, and the configuration verified to ensure this is optimal for the system requirements.



Networking

Critical to any IT system is the network providing connectivity to the system for end-users and connectivity to other IT solutions for integration.

The Claremont Infrastructure Health check will look for and identify any areas for concern such as dropped packets, saturated links, latency etc. It will also verify whether the TCP stack is optimized effectively for the system workload, e.g. high throughput or low latency.

Note this configuration is isolated to the server operating systems only. It is not expected that the Claremont consultant will require access to firewalls or other networking peripherals.

Performance

Performance is an exceptionally complicated area where commonly an "ideal" performance configuration is impossible given the varied nature of system load with most IT systems. The goal here is to ensure that the IT system is configured optimally for the load profile applied to it, weighting this configuration towards more time-critical activity and away from those activities where time pressures are not so prevalent. Inevitably there is a trade-off.

The Claremont Infrastructure Health Check investigates the following areas:

- CPU activity
- Memory usage & paging
- IO utilization & throughput
- System wait time
- Log file reviews (e.g. dmesg & /var/log)

In addition, the system is reviewed to investigate configuration such as the IO Schedule type (deadline, CFQ, NOOP etc.) and, if available, longer-term statistics are reviewed to identify any changes in performance & capacity requirements over time.

Security

Like performance, security is a vast area where there are many conflicting opinions as to what constitutes effective systems security. Claremont has drawn upon its consultants' cumulative experience of IT systems management to define some key areas to investigate. These are:

Systems Access

- Software firewall configuration (e.g. iptables)
- PAM (if applicable) password policies etc.
- Ensure no remote root login
- Remove/lock unused accounts
- Ensure leavers/movers process includes locking/ removal of user accounts

Intrusion Detection

- Review IDS configuration (passive/active)
- Review auditing configuration
- Log file review to ensure activity is being captured
- Review, if relevant, any FIPS/FIMS configuration

Intrusion Prevention

- Review software firewall configuration
- Review WAF configuration (if relevant)
- Review relevant logs pertaining to intrusion prevention

System Patching

- Ensure robust patching strategy
- Identify any required patches for security flaws

General Secure Configuration

- SELINUX – can provide a higher level of security for an admin overhead
- Review active services – inactive services should be disabled/uninstalled
- Review encryption strategy to ensure data both in transit and at rest is encrypted where appropriate
- Check configuration security – e.g. password access for kernel boot
- Review user configuration limits

Conclusion

The above represents a thorough review of system configuration. However, no two IT systems are alike and there may be other areas the consultant reviews and investigates to augment the Health Check.

Commonly customers require further reviews of systems with regards to Cloud Migration Readiness, including a review of licensing, performance, security and service requirements. This may support a process to decide whether to move to Cloud or help prepare for a planned move to the Cloud.

This can be further extended to include specific application requirements, e.g. Oracle Database and e-Business Suite patch levels recommended for Cloud-based solutions.

This will be discussed on-site with the relevant support personnel to identify and agree to these areas.

Choosing the Right Managed Services Provider

If you are looking for an Oracle partner who can help you with your Oracle Infrastructure Health Check, goes about it the right way and can back up the talk, then contact us.