ZYNSTRA TECHNICAL BRIEFING NOTE

iLO Out-of-Band Management

Introduction

Every Cloud Managed Server has a dedicated physical out-of-band management interface called an iLO (integrated Lights Out) network interface. This is not required during normal operation, administration or monitoring as these activities are all carried out using the outbound OpenVPN management VPN that servers initiate as they connect to the Cloud Management Platform. The iLO is only needed in exceptional circumstances where a serious software error has resulted in a loss of WAN and/or management VPN connectivity, in cases of hardware component failure or for operations such as powering off or starting a clustered Cloud Managed Server from cold.

The iLO capability is provided by the HP hardware and firmware upon which each Cloud Managed Server is based and as such is separate to the virtualised software running on the server, In fact, it would not offer true out-of-band management if it were not. On the rare occasions when it is needed, it is useful for the Customer Success Team to be able to access the iLO remotely in order to ensure investigation and resolution of issues is as fast as possible. The iLO also provides significant, low-level access to the server so it is important that it is secured.

The iLO has some built-in security features that are always enabled. For example, there is a logon rate limit imposed by the iLO. Every Cloud Managed Server is configured with a unique, non-default username, and a unique, complex password. These credentials are stored securely, in encrypted form by the Customer Success Team. These measures should ensure that a remote brute-force or dictionary-based attack should both be nearly impossible. The iLO firmware is also kept up-to-date to minimise the risk of a security vulnerability in the iLO implementation itself. iLO access attempts are also logged in terms of username and source IP. However, the iLO does not have a built-in firewall itself to limit connections by source IP.

Connectivity Options

Some iLO connectivity options, along with their pros and cons, are listed below. The choice will ultimately depend on personal preference, any regulatory or security compliance requirements and the technical environment that the server is being deployed in.

- **iLO with either a public or private IP, and a 3rd party firewall in front that can restrict traffic to a whitelist of IPs.** The firewall does not need any sophisticated capabilities other than the ability to restrict traffic via source IP and in the private IP case, allow inbound port forwards to be configured (note that it is not possible to use the server itself to achieve this - although it has these capabilities, iLOs are required precisely in situations where the virtualised software may not be running). This would involve purchasing, or repurposing, and configuring a simple hardware or software firewall to protect just the iLO, via a source IP whitelist of IPs

that can connect. This option provides full protection and continuous remote access to the iLO, but potentially involves some cost to purchase and maintain the firewall. In a double-NAT scenario, there may well be no need for a separate 3rd party firewall, if the firewall upstream of the Cloud Managed Server has source IP restriction capability.

- **iLO with a public WAN IP, and directly connected to the router/public Internet.** This option means that the iLO is contactable from any IP on the Internet, though the security features mentioned above would still apply. It has the advantage that the Customer Success Team has continuous iLO access, and a separate firewall is not needed, but it is potentially not as secure.

- **iLO with a public WAN IP, but left it unpatched (air gap) from the router/public Internet.** The iLO needs to be physically patched in when needed, and left unpatched when not. This offers increased security compared to having it permanently connected, but involves manual effort to do the patching by the end customer, and a potential for delay while this is done if there is a service outage (SLAs consequently would not apply) since there is no continuous remote access for the Customer Success Team.

If you are responsible for the ILO connection and are considering the options above, please do not hesitate to contact the Customer Success Team for assistance/guidance or visit the Support Portal.