BEST PRACTICES FOR MANAGING IDRAC SERVICE PROCESSORS

OVERVIEW

Securing and Maintaining iDRAC networks

Service processors such as the Dell EMC iDRAC have done much to improve administrators' ability to remotely access and monitor servers rapidly and efficiently. They are truly powerful tools that, when not properly maintained or configured, can create a dangerous backdoor into IT equipment. Most recently, security researchers have encountered hundreds of thousands of misconfigured and unpatched service processors attached to production networks[1]. In many cases, these service processors were accessible from the public Internet, with tens of thousands using default passwords or outdated firmware with known vulnerabilities. Any user with malicious intentions could, with little difficulty, assume complete control of these servers remotely.

Mitigating the Risks to your Service Processor

Regular patching and failure to configure

As the recent heartbleed bug demonstrated, even the most scrutinized code can include very serious bugs. Also, while many vendors offer continuous maintenance releases for their service processors, most data centers do not have policies to enforce patch management for service processors.

A larger issue than a lack of patching is connecting the service processor to the network without changing the default configurations. Default configurations on service processors are well known in the industry, and a lack of changing these can give anyone with network access complete control of a server.

Unauthorized network access to service processors

Many data centers simply treat the service processor as another network port that is plugged into the production networks. According to recent research, over 300,000 servers have their service processors accessible from the public Internet[1]. Countless more are accessible to normal users from their internal networks. Views on users are changing; for example, new specifications being drafted for government IT security have started assuming that every user is a potential threat. This underlines the thought that limiting the potential for unauthorized users' access is always a good idea.

Common Solutions

Network Isolation

This is the most effective method to ensure service processor security is using an "air gap" between your production network and your maintenance or service processor network. This approach is very effective; however, it requires extensive network configuration. Basically, you will be creating a completely new network.

Centralized Authentication

Proper system security requires that all sessions are authenticated, authorized and logged. The most convenient way to achieve this on most systems is by using a central directory system such as LDAP and ActiveDirectory® and a central Syslog server. This approach requires the manual configuration of directory and Syslog settings of each iDRAC.

VERTIV. DELL EMC

[1] *Farmer, Dan. "ipmi: freight train to hell" Published: August 12th, 2013 Accessed: May 19th 2014. http://fish2.com/ipmi/itrain.pdf*

Streamlining Service Processor Security and Access

Network Isolation with Avocent® Universal Management Gateway

The Avocent® Universal Management Gateway appliance protects iDRAC by creating an isolated service processor network. The isolated network is protected by a hardened Linux distribution with complete access control (directory authentication, access control and logging). The appliance aggregates all iDRACs and presents the main iDRAC functions (console, power control, sensors, etc.) in a user-friendly single pane of glass view. Up to 40 iDRACs can be connected to each appliance.

Secure Centralized AAA[2] Deployment

The Avocent® Universal Management Gateway appliance is a perfect companion for a well thought out AAA[2] Security strategy. It seamlessly interfaces with your existing authentication LDAP ActiveDirectory® infrastructure and eliminates the need of having to maintain usernames and passwords on each iDRAC. With the appliance, you can simply specify what LDAP/ AD groups have access to the iDRACs, and the Avocent® Universal Management Gateway appliance will do the rest.

Rapid deployment

More importantly, the Avocent® Universal Management Gateway appliance is the most efficient path to rapid and secure deployment of Dell EMC servers with iDRACs. The appliance will auto-detect new iDRAC servers connected to it and immediately populate the new server in its Data Base, providing instant secure access to the powerful management functions within the iDRAC.

Avocent® Universal Management Gateway

[2] *AAA: Authentication (LDAP/AD), Authorization (LDAP Groups and schemas) and Auditing (Syslog)*

VertivCo.com | **Vertiv Headquarters,** 1050 Dearborn Drive, Columbus, OH, 43085, USA

GSC-DELL-052 (R09/17)