The Environmental Concerns of Remote Data Centers...

Inside and Out

The proliferation of far-flung data centers is necessitating smarter approaches to keeping those networks resilient.

By Gary Marks

It seems like every month there's another announcement of a data center popping up in an unusual locale. Perhaps the most recent case in point: Microsoft is moving forward with plans to put a data center deep down in the Pacific Ocean, pending an environmental study. Both the location and the environmental care taken make sense; data centers produce a great deal of heat and require tremendous amounts of power to operate and to cool. (And, unfortunately, water usage, pollution, power derived from non-renewable sources, and similar concerns broaden the picture of this impact.) The environmental effects of data centers – especially in the context of global climate change – are a driving factor in choosing some of these more remote locations.

A good number of these unusually placed data centers use the natural climate (i.e. the cold of the Arctic Circle) to their advantage. However, it's important to notice the special emphasis put on ensuring the environments inside data centers remain hospitable to their most valued residents: the networking hardware within. For example, Facebook's data center in Lulea, Sweden cleverly uses arctic air to cool its servers, but is careful to first treat the air with water vapor to achieve the correct humidity for the equipment. In neighboring Finland, Google built a data center near the Gulf of Finland to make use of its freezing waters. Doing so cools servers without relying on refrigerants, with water converted to fresh water (and back again) in order to protect equipment. By virtue of its altitude atop the Swiss Alps, the Deltalis RadixCloud data center gains cold air and water to cool equipment – and because the location is a former Swiss Air Force base, security and reliability aren't issues. Finding the same advantages not on top of a mountain but below one, data management company Iron Mountain burrowed its main data center deep underground within a limestone mine in Pennsylvania. Trusted by government agencies and companies with highly sensitive data, the center's equipment lines limestone tunnels able to handle heat.

While there are plenty of reasons for putting data centers far from the center of operations – from security to cost to environmental responsibility – doing so requires some forethought. For most companies relying on data center resources, it's critical to maintain the uptime of that equipment, and to be able to remotely access and troubleshoot equipment when issues do occur. Without remote access to far-flung networking hardware, an outage can mean expensive and time-consuming international travel, all to get a technician to one of those exotically located data centers to fix what might end up being an unplugged cord.

As an example, reliable access to remote, critical IT was a scenario that Mass-based Interactive Motion had been all too familiar with. The medical device company regularly needs to service its InMotion therapy robots at hospitals around the globe, and traditionally would suffer the costs and burdens of sending personnel abroad whenever an issue occurred. It has since switched to remotely monitoring and managing the technical well-being of the robots via cellular connections, eliminating technician travel requirements.

Whatever the issue and wherever the networking equipment, the cost of downtime is becoming increasingly staggering. Any outage means lost revenue, which Gartner pegs as averaging a cost of $5,600 per minute of downtime. And, that estimate doesn't factor in the potentially greater costs that come with long-term reputational damage to a business.

Remote access to data center equipment is critical to reducing network downtime and maintaining business continuity. Businesses should also seek out the inherent resilience that comes with redundant methods of remote connectivity and capabilities for out-of-band management. With global climate change comes the possibility of increasingly severe weather – and storms, flooding, fire, and temperature extremes are devastating threats to network hardware and connections. Out-of-band management means being able to access hardware even when a primary connection is offline, and utilizing a diverse secondary connection method can mean the difference between having resilient access and, well, not having it.

Take, for example, a case where hardware includes both a landline and a backup cellular connection. A storm may knock down lines and take the landline offline, but the cellular connection will take over and the business's customers will be none the wiser that there's any issue.

As a part of achieving network resilience, it's important to be able to remotely monitor the environment within the data center as well. Network hardware can be equipped with sensors for temperature, humidity, smoke, flooding and more, and set up to provide automatic alerts when these sensors detect trouble. In many cases these alerts can save the day and maintain uptime, giving technicians the heads up to remotely power down overheating systems or reroute connections. In the same way, network hardware with automatic remediation capabilities for handling these and other similar scenarios can safeguard equipment and uptime by addressing issues quickly, without waiting for technicians to take action. Technicians can set customized rules and policies that tell equipment which automatic actions to take when defined events occur, empowering hardware to act as a robotic caretaker that is always on the scene and vigilant in protecting the local environment.

With the concern for the earth's environment growing and with extreme weather threatening data center connectivity (along with plenty else), businesses are finding ways to maintain network resilience by safeguarding the environment within the data center, while taking steps to lessen their impact on the world as a whole. ■

Gary Marks is the President of Opengear, a company that builds remote infrastructure management solutions for enterprises. Opengear has Executive offices in Piscataway, NJ. Follow Opengear on Twitter: twitter.com/Opengear