

A Plan Comes Together – The Oregon Department of Education Data Center Move Project

Background

In November 2003, the Oregon Department of Education (ODE) was operating forty-three (43) aging servers on shelves and under desks with local or direct attached storage, a poor backup software/strategy, and very little control over administrative access except for the database servers. This general disorganization resulted in frequent unplanned downtime, potential loss of data, and a network team that operated in reactive mode only. The worst result, though, was a reaction from the customers, who had very low confidence in the availability of the ODE network and its resources.

By late 2004, ODE had consolidated its server footprint down to twenty-two (22), established backup policies and procedures, centralized command and control of the servers, implemented a storage area network (SAN), and installed health monitoring software. The agency was also able to eliminate the need for several software applications by leveraging features available in the updated network operating system. The result was a total savings of approximately \$250,000 per biennium in hardware and software maintenance and replacement costs, and a network team that was beginning to operate in a proactive manner.

Although ODE had come a very long way in one year, the agency also began to recognize early on that it would need to find a more suitable location to house its hardware to address remaining issues. The Public Service Building (PSB) where ODE is located was built in a ten-year period between 1938 and 1948. Even though the HVAC had been updated thoroughly, it was still less than adequate or desirable for the needs of ODE. In 2008, there were at least four separate incidents in a single month when the cooling went out completely; ODE administrators had to come in and shut down all non-essential systems and call maintenance.

Synopsis

In 2005, the State of Oregon launched a Centralized Network and Infrastructure Consolidation (CNIC) project. The idea was to take the twelve (12) largest data centers in state agencies and consolidate them into a single centralized State Data Center (SDC) to be built at a new location. While the Oregon Department of Education was very interested in consolidation and moving its servers to a state-of-the-art facility, the agency also had concerns about potential security and Family Educational Rights and Privacy Act (FERPA) compliance issues associated with colocation in a data center managed by staff who were not State Education Agency (SEA) employees.

The Oregon Department of Education posed the question to the Family Policy Compliance Office (FPCO). **Could ODE allow servers housing student-level data to reside in a shared facility staffed by personnel who were not employees or contractors of the SEA, knowing that these individuals would have full**

administrative access to said servers? In May of 2007, the FPCO responded with a decision that is best summarized by the following excerpts from their formal letter:

Based on the information you have provided, we conclude that SDC staff do not qualify as “authorized representatives” of ODE under 99.31(a)(3) of the FERPA regulations because they are not employees or contractors under ODE’s direct control. ... Therefore consolidating ODE data into the SDC in the circumstances you described would not meet FERPA requirements, and we are aware of no other exception to the consent requirement in FERPA that would permit ODE to re-disclose personally identifiable information from education records to SDC staff.

Even though ODE had determined it would be unable to move into the SDC, the Department still required a better location to house its leading edge data center. The agency began looking for suitable alternatives to house the equipment and found what seemed to be a perfect prospect.

In 2003, the Oregon State University (OSU) had begun to build the Open Source Laboratory (OSL). The facilities were state-of-the-art, and the location in Corvallis was only thirty-four (34) miles away from Salem. Also, OSU staff were already trained on, and compliant with, FERPA. Since there were discussions about how the Oregon University System (OUS) would be able to use some of the data from the newly developed ODE statewide longitudinal data system (SLDS) for their research, it seemed to be a perfect fit physically and logically for the Oregon Department of Education as well as a big step toward forming a more productive partnership with OUS.

The Plan

In September 2008, ODE applied for a SLDS grant through the Institute of Education Sciences (IES). As a part of this project, ODE specified that it would colocate its data center at OSU’s Open Source Lab. ODE was awarded the \$3,696,615 grant in early 2009. The first formal technical planning meeting for the data center move project was held on October 9, 2009. There were technical staff in attendance from: ODE, OSU, the Network for Education and Research in Oregon (NERO), and the Oregon Department of Administrative Services.

During the technical planning meeting, it was decided that ODE would purchase and install its own firewalls so that the agency could operate a secure encrypted Virtual Private Network (VPN) tunnel between ODE’s location in the PSB and the OSL (Figure 1).

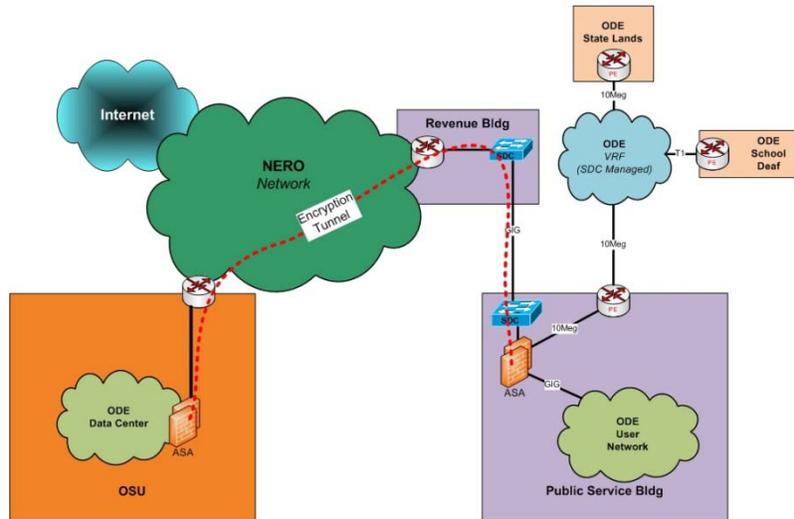


Figure 1

The server move would require ODE’s application development staff to manage servers that were no longer at their same physical location. Developers would be moving large amounts of data from their workstations at the PSB to the servers at OSU frequently. This would require the VPN tunnel to support at least one gigabyte (1GB) of bandwidth throughput, and the firewalls would need to be redundant to eliminate single points of failure. This meant purchasing four large firewalls and placing two on each end of the tunnel in failover mode (Figure 2).

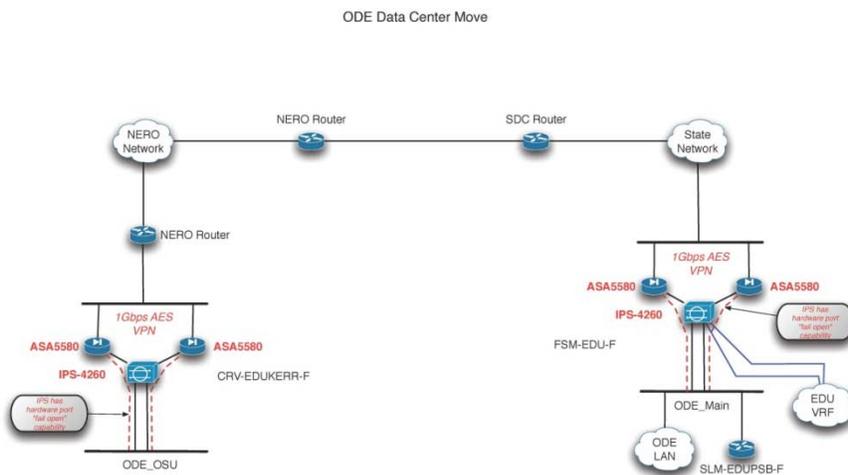


Figure 2

ODE decided to execute the project in three phases. Phase I entailed replacing all of the existing closet switches at the PSB with 1GB power over Ethernet (POE) switches while also taking the opportunity to install a flexible, professional, and secure wireless network.

The physical portion of the data center move would be Phase II. The Department's Storage Area Network (SAN) and all but a handful of the servers would be moved to the OSU Open Source Lab in Corvallis, Oregon. This physical move would also result in a new internet service provider (ISP) for the agency, NERO.

Although months were spent planning the move, the actual execution of Phase II took only twenty (20) hours. This included shutting down all equipment, un-cabling, un-racking, packing, loading, transporting, re-racking, re-cabling, and powering all equipment back up. When the equipment was powered up and tested, all of the systems and new firewalls were fully operational and no additional modifications or corrections were needed.

Phase III involved migrating the user networks at each of the three existing sites (PSB, Oregon School for the Deaf, and the Oregon State Lands Building) from their current ISP (the State of Oregon) onto NERO.

This phase held the most risk, as failures would cause downtime for services that are critical to the agency and the public; such as losing the ability to access the Law Enforcement Data System (LEDS) that allows ODE staff to do background checks on bus drivers, or losing access to financial systems required for regular payments to school districts. Due to the high risk, ODE felt it was safer to separate this phase from Phase II by several months, so that technical staff had more time to test and mitigate the risks.

The Pros and Cons

As with any business decision, ODE had to weigh the pros and cons and then make the right decision based on the Department's priorities. Some of the pros and cons for ODE concerning the data center move were:

Pros

- Improved business continuity and reduced downtime – reliable facilities, adequate cooling, redundant and sufficient power
- Increased span of control – ODE controls its own firewalls
- Faster network access – increased bandwidth and the potential for better peering through a new ISP (NERO)
- Segmented network traffic – different points of presence for internal user traffic to/from internet and external user traffic to/from servers
- Data collocation for research – Oregon University System facility which postures ODE, both physically and politically, to begin working more closely with the OUS

Cons

- Increased responsibility – ODE controls its own firewalls
- Increased risk – many risks involved (see below)

- Increased costs – offset in the short term by federal grant
- Required downtime – all ODE services would be unavailable during the data center move
- Increased travel – added inconvenience for data center access due to remote location
- The UNKNOWN

The Risks

The ODE Data Center Move Project had the potential to be a disaster of extreme proportions. Every project has risk, and there were a plethora of risks on this project. ODE was relocating over one million dollars (\$1M) worth of equipment, over seven terabytes (7+TB) of data, and hundreds of custom developed applications with tens or even hundreds of thousands of development hours invested in them.

There were also many other unique project challenges:

- ODE project manager had never managed a project of this scale, or one involving so many external vendors and partners.
- ODE had a very small technical team of three people, actually only two, as the team lead was also the project manager.
- Of the remaining two people, one of them had only been with the agency for a short time. In fact, he was brought on while the project was in process.
- ODE was introducing new and extremely complex hardware that no one on the team had ever managed or configured, such as enterprise firewalls and intrusion prevention systems.
- ODE's equipment was moving to a location forty-five (45) minutes away, which meant routine maintenance and break-fix procedures needed to change. The network/server team would no longer have its hardware in the room next door.
- Application development teams were concerned about the servers being so far away from them, specifically concerns on management accessibility and application performance.
- Ensuring security of the data regarding compliance with federal and state regulations.

When coupling the risks above with the existing risks of any normal data center move, it becomes obvious how daunting this project seemed at first. However, the trick to dealing with risks is to acknowledge them, understand them, plan for them, but don't let them consume the project. Not concentrating on risk allows for concentration on the project.

The Results

Phase I

ODE normally reserves two hours a week for network/server maintenance downtime. Phase I of the ODE data center move was conducted during this scheduled downtime across two successive weeks. During this time, ODE replaced twelve (12) one-hundred megabit per second (100Mbps) local area network (LAN) switches, with twelve (12) one-gigabit per second (1Gbps) POE switches.

ODE also added two Cisco wireless controllers and ten (10) Cisco wireless access points (WAPs) during this time period. These replaced customized consumer grade WAPs, adding a greater level of security and giving ODE a professional wireless presence for visitors and internal staff alike.

Phase II

Phase II consumed approximately sixty percent (60%) of all planning time and entailed the largest physical and technical portion of the move.

At 6:30 a.m. on August 20, 2010, ODE technical staff came in to work and began shutting down all of the servers, the SAN, and the other network devices in the racks in the Public Service Building. Dell technicians showed up at approximately 8:00 a.m. to begin un-cabling and un-racking all of the equipment. At about the same time, the moving company also arrived and began professionally packing all of the hardware for its journey down the freeway to Corvallis.

By 1:30 a.m. on August 21, 2010, just 19 hours later, all of the equipment had been re-racked, re-cabled, and was in fully operational status. Members of the ODE Outreach team arrived at approximately 9:00 a.m. on the 21st to test the applications for functionality and availability and found no problems. This was a major milestone for the Oregon Department of Education.

Phase III

Due to this being the riskiest phase, an extra four months was spent preparing to move the user networks. The end result was actually somewhat anti-climactic. The senior network administrator and the Chief Information Security Officer (CISO) came to work on January 2, 2011 at 9:00 a.m., and by 9:15 a.m. the agency was switched over. There was an additional forty-five (45) minutes of testing and the change was complete.

The ODE network/server team thought there might be a few minor issues to resolve in the days following the network change, but there was a grand total of one issue. Just one issue, and as it turns out, that one issue happened to be a firewall connection that belonged to another agency.

What Worked and Why?

Opportunity

This project began with opportunity. As with any project, there was the opportunity for success or failure. There was also the opportunity for increased partnership with higher education (OUS). There were many other opportunities; such as building new relationships/partnerships, the opportunity for vendors to sell their products, the opportunity for those hungry for knowledge to learn, and the opportunity to lead. All of these opportunities boiled down to one thing: motivation, and motivation is an essential tool in leadership.

Stakeholder Buy-in

This was another big key to the success of the project in every aspect. From the inception of project planning stages, to supporting the needs of the project, the stakeholders played a major role in the success of the data center move.

ODE management stayed closely aligned with technical staff and ensured that staff had all of the resources that were needed to do the job. Biweekly status meetings were held between the project sponsor, the network manager, and the project manager to quickly address any barriers.

Leadership

From the infancy of the project's planning stages to supporting the needs of the project, leadership played a major role in the success of the data center move. The leaders in this project were more than just leaders; they were truly "enablers."

Individuals in leadership roles enabled everyone, from the lowest ranking technician to partners and even vendors, by believing in them. ODE leadership never expressed doubt in those working on the project, they only displayed confidence and trust in everyone involved. This kept the project on a positive note at all times, even when timelines and resources were tight.

Instead of trying to manage or micro-manage the project themselves, project leadership simply trusted everyone to do their job and spot checked work on the project.

Relationships/Ownership

More than anything else, the relationships that were developed and the ownership that was established formed the core of the project. The relationships in this project were varied, complex, and unfamiliar. There were several entities involved in the project, and ODE had not worked with the majority of these organizations previously.

The key to solidifying these relationships was making sure that all of the major parties involved were a part of the process from the very beginning. Not only was it necessary to involve some of parties early on in the project for planning purposes, but it also ensured their buy-in to the outcomes of the project as well. This involvement facilitated input from the parties which in turn fostered a sense of ownership in the success of the project. This was especially applicable to the Oregon State Data Center and the Oregon State University; but involving other parties, such as vendors and service contractors, and treating them as partners was also a critical factor in the success of the data center move project.

Summary

There were a myriad of factors that made this project a success: good planning, state-of-the-art technology, proficient training, ample resources, tenacity, persistence, and maybe even luck. But the real key to the success of this project comes down to one simple thing and that thing is people.

When planning a similar project, it would be wise to consider the following factors to be successful:

- Give yourself plenty of time to plan and involve all of the key players. One person cannot think of everything.
- Spend more time than normal on your risk mitigation plans. Get input from all key players.
- The project manager should spend as much of their time managing relationships as managing the project.
- Turn your vendors into partners. Give them buy-in to the project and make sure they know that you value their opinion. Vendors have resources, such as system engineers, at their disposal to ensure that they succeed, which in turn will make your project successful as well.
- Buy the best product(s) you can afford for your project and plan for future expansion. Have a vision.

Finally, there is no replacement for getting the right people to invest and care about the success of the project. Open and honest communication between all parties is also critical. Good communication between the right people will compensate for short-falls in other areas, but nothing will be able to compensate for poor communication between the wrong people.