semperis

CASE STUDY PRIME HEALTHCARE

PRIME HEALTHCARE REDUCES DISASTER RECOVERY TIME FROM DAYS TO HOURS WITH SEMPERIS ADFR

Semperis ADFR is the "pinnacle" of California-based healthcare organization's disaster recovery plan

A planned internal change that fell short of expectations prompted David Yancey, Senior Systems Engineer, to completely overhaul Prime Healthcare's entire Active Directory disaster recovery plan. During routine maintenance, storage that contained many of the organization's domain controllers was accidentally deleted.

That incident highlighted a critical problem for an organization that runs 45 acute-care hospitals in 14 states: The time required to restore domain controllers was too long. Every minute that systems were offline increased the risk to patient safety.

"Active Directory is our main source for user authentication for mission- and patient-critical applications," said Yancey. "If AD goes down, it means a complete outage. Our hospitals would struggle without access to their EMR (electronic medical record) applications. It would be extremely challenging."

Yancey's search for a faster, more efficient AD recovery method led him to Semperis Active Directory Forest Recovery (ADFR), which he said has accelerated the organization's recovery time by orders of magnitude.

"Basing off the worst-case scenario, with ADFR it would now be about 24 hours to completely recover—including cleaning up the metadata—at the most, compared to the previous process, which would take days," he said. "Especially in our environment, with over 100,000 user objects. Doing the direct restore via ADFR backup is a lot quicker."

The recovery process the organization used before implementing ADFR was painfully cumbersome.

"If we had an absolute disaster, we would restore all DCs within a 24-hour window, then we would do what we could to make sure that verification was working with every single one of those domain controllers," said Yancey. "In some cases, we would have to create new ones, which took a lot of time. We knew we could do better."

SEARCHING FOR FLEXIBLE BACKUP TIMING

As part of Yancey's mission to rewrite the organization's disaster recovery plan following the deleted-DC incident, one of his first objectives was to find a solution that would accommodate flexible backup windows and allow backup management to remain in-house.

SEMPERIS ADFR IS ESSENTIAL TO PRIME HEALTHCARE'S DISASTER RECOVERY PLAN

- Reduces AD recovery time from days to minutes
- Accelerates routine backup processes
- Provides isolated recovery test environment
- Offers flexible backup scheduling for the organization's 45 hospitals
- Enables delegation of backup management with easy-to-use wizard and comprehensive documentation
- Helps comply with regulations by underpinning documented DR plan

ABOUT PRIME HEALTHCARE

- California-based healthcare organization with 45 acute-care hospitals in 14 states
- 50,000 employees and physicians
- 2.6 million patient visits annually

"Having ADFR at the center of our DR plan put my mind at ease because now we know that if an incident happens again that takes out the DCs, we have a direct course of action to take.

David Yancey
Prime Healthcare Senior Systems Engineer

"To get a really good backup of our entire environment, everything has to happen in a certain window," he said. "We kept having issues with successfully completing backups within that window. And our team wasn't comfortable with a third-party solution."

Semperis ADFR offered a flexible, fast solution for AD backups, comprehensive documentation that empowered other team members to manage backups, and confirmation messages that gave Yancey and his team peace of mind.

"The ability to restore multiple domain controllers at once in the database is the thing we were going for, and also the cleanup of metadata," said Yancey. "And ADFR sends me emails every day letting me know what is backed up. I'm able to just set it and not be constantly monitoring it. ADFR is backing up everything according to the backup windows that are tailored to our particular regions."

Yancey said that nearly every aspect of ADFR simplifies the AD backup process, which in turn saves time and resources.

"The ability to just restore everything within ADFR's wizard panel—that's very important," he said. "I'd been doing restores manually in the past. Even when you use PowerShell, it's cumbersome. Another important aspect of ADFR is that if I'm unavailable, other people can take over because it has thorough documentation."

One other ancillary benefit of ADFR is that it has eliminated DC backups outside the main data centers, which speeds backup times during the designated time periods.

TESTED DR PLAN BRINGS PEACE OF MIND

Before implementing ADFR, Yancey wasn't confident in his ability to restore AD quickly. But now that he can use ADFR to stand up an isolated test environment, he conducts test restores biannually and after every application upgrade.

"Having ADFR at the center of our DR plan put my mind at ease because now I know that if an incident happens again that takes out the DCs, we have a direct course of action to take," he said. "Before implementing ADFR, I was having a lot of issues trying to restore a secure channel between AD and the other previous restores. But now—since I've tested it multiple times—in the event of a disaster, we know exactly what to do."

Another plus to the test environment: Having a tested and documented DR plan also helps the organization comply with myriad regulations regarding patient data.

DEFENDING AGAINST CYBERATTACKS AND HUMAN ERROR

Yancey said that although most organizations—including Prime Healthcare—are hyper-focused on defending against cyberattacks because of escalating and highly publicized incidents, guarding against human error is just as important. He now feels confident that Prime's documented DR plan will protect the organization in the event of an outage regardless of whether it's the result of a natural disaster, a cyberattack, or a simple mistake.

"It's one thing that you don't expect to happen, and then it happens," he said. "Prime has spent millions of dollars on improving security posture, implementing solutions to detect malware, and running through malicious attack scenarios. But there's also the factor of the access that people have, or it's simply an accident. Those probably contribute most to the overall risk profile."

ADFR: THE "PINNACLE" OF THE DR PLAN

After implementing ADFR and evaluating its contribution, Yancey now considers ADFR an essential part of Prime Healthcare's DR plan.

"It's the pinnacle of our recovery plan," he said. "It's one of the top things that any company in the healthcare field should have. When doctors need access to patient records to deliver care, we have to be able to restore as quickly as possible. ADFR is invaluable."

"ADFR is the pinnacle of our recovery plan. It's one of the top things that any company in the healthcare field should have."

ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference (www.hipconf.com). The company has received the highest level of industry accolades, most recently ranking as the third fastest-growing cybersecurity company on the Inc. 5000 list. Semperis is accredited by Microsoft and recognized by Gartner.