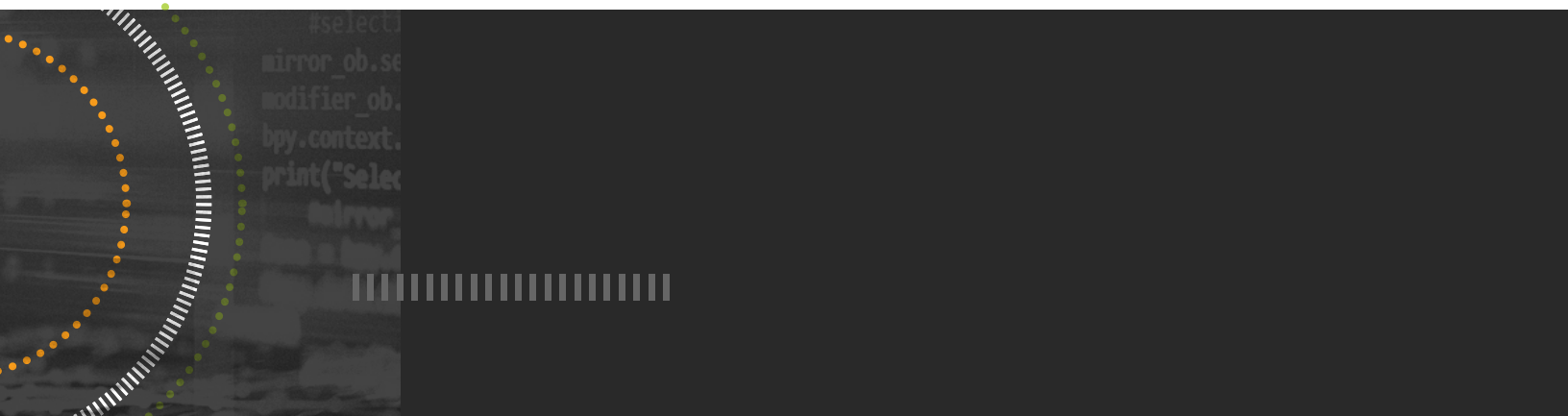
solarwinds

WHITEPAPER

Active Directory: 3 Reasons You've Forgotten Why It Still Needs Monitoring



Active Directory: 3 Reasons You've Forgotten Why It Still Needs Monitoring

When thinking about keeping the business running, your mind usually goes to critical workloads, the lifeblood of your organization. It could be a customer-facing web application, a back-end database, or a mobile application platform. But at the heart of most organizations still lies Active Directory (AD). Even with most orgs likely running in a hybrid AD environment, on-premises AD still represents the foundation for all the organization's productivity and security.

And with the expectation of businesses always being available to employees, contractors, partners, and customers, the need to be up and running reaches all the way down to AD. In many cases, if AD isn't running, the impact upon applications and resource access—both on-premises and in the cloud—can be greatly magnified.

OK, so keep AD running, right? Sounds simple enough, but the reality is without monitoring certain parts of AD to see if it's running—and running *well*, IT organizations assume AD is always going to be there and just *do its thing*. And, if you stop and think about it, because AD has been around for nearly 20 years, there's the assumption it's *just going to work*.

But like any critical workload on which your operations depend heavily, it's necessary to put specific monitoring in place to be certain your trusted AD isn't giving out on you. This is something you've known for years. But, like most IT pros, the lure of newer and more exciting technologies has taken your focus away from AD and caused you to forget AD itself is the most critical service you offer and you need to ensure its availability, security, and performance.

In this whitepaper, we'll look at three forgotten reasons why Active Directory requires monitoring. With each, we'll provide details on what specifically needs to be monitored and provide guidance on how to best do it

SolarWinds Insights: Server & Application Monitor

Your environment is a multifaceted mix of systems, applications, platforms, and services—of which, AD plays a major role. But as your environment grows and changes, IT can't just add on *another* monitoring tool.

SolarWinds *Server & Application Monitor* and *Log Analyzer* centralizes the monitoring of your entire environment, bringing insight into the current and changing state of every aspect of the network. Look for insights from SolarWinds throughout this paper.

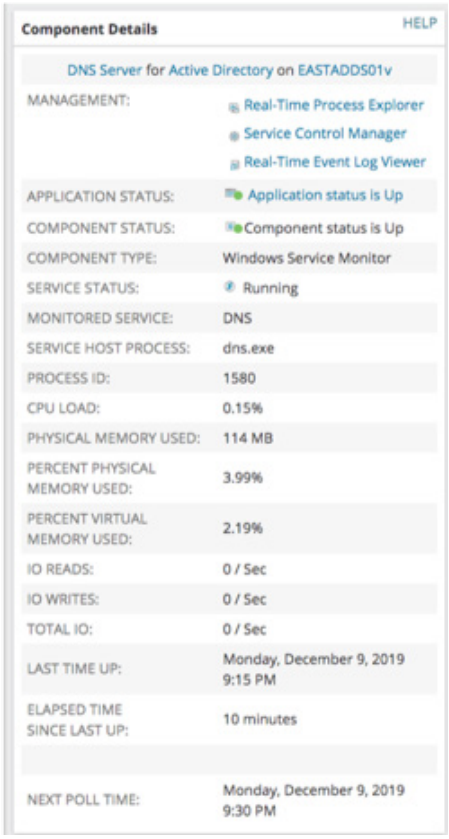
Reason #1: Your AD Should Have a Strong Foundation

AD is an application running on Windows. This means there are countless reasons outside of AD potentially causing it to fail. The simple example of a rogue process eating up all the CPU utilization on one of your key DCs could be the source of multiple problems within AD. It's important if you're planning on monitoring AD itself, you first be mindful of monitoring the underlying systems and services on which AD rests.

There are a few specific foundational aspects of your environment impacting whether AD is running and, therefore, should be included in your AD monitoring strategy:

- **DNS** – AD can't run without DNS, so monitoring of DNS and its services are a given. Being sure the Windows service controlling DNS is running and the AD-related zones are intact, is essential.
- **SolarWinds Insights: Monitoring DNS Health** Because of its foundational responsibility to the success of AD, monitoring of DNS involves more than watching to see if the DNSServer service is running or not. SolarWinds® Server & Application Monitor seeks to have a comprehensive view of the server hosting DNS, the DNS service itself, and the performance relationship between the two.

  By monitoring the service and host system (as shown at right), Server & Application Monitor can better understand whether an issue lies with the DNS service itself or the system on which DNS resides.
- **Directory Services in Windows** – Make certain any Windows services related to AD are configured properly and in a Running state is the first step to ensure AD is operational.
- **Windows Server Performance** – The systems designated as Domain Controllers (DCs) are still Windows servers at the end of the day. Monitoring these servers for system performance, resource utilization, and even hardware health helps to ensure you're well in front of any potential issues outside of AD potentially bringing it down.



Proper AD performance relies on good AD health which, in turn, is dependent upon foundational services and systems running well. By including these as part of your monitoring, you ensure your picture of the health of your AD is truly "bottom, up."

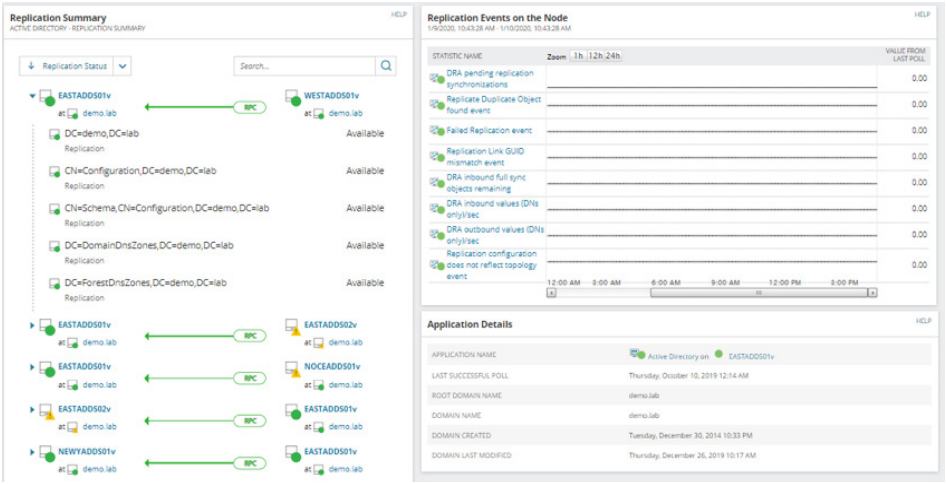
Reason #2: AD Performance Relies On a Lot of Moving Parts

AD is by no means a simple service. It's a complex combination of databases, services, roles, replication, communication, ports, security, and connectivity—all bundled together to seamlessly provide an environment with productivity and security.

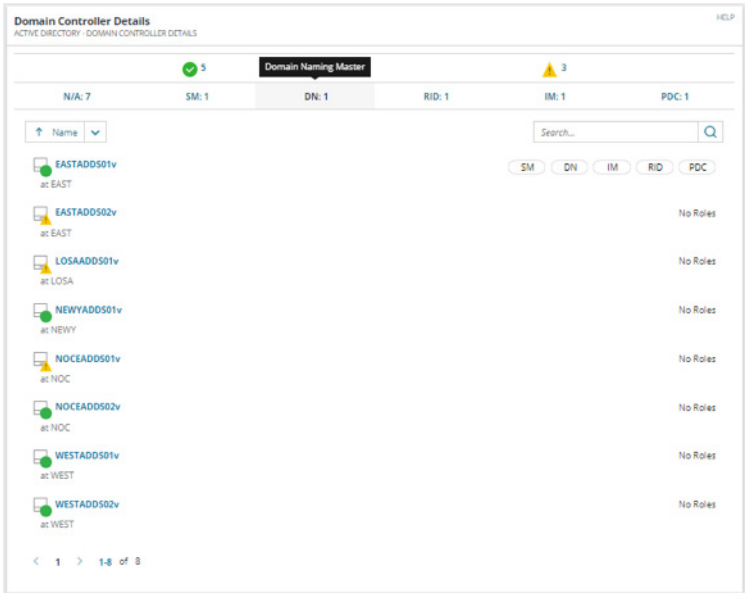
Several parts of AD can (and do) change on a daily basis and may be the root cause of larger operational issues. These should be included in your monitoring list and include:

- **AD Replication** – Out of sync DCs can result in a wide range of issues, mostly revolving around an inability to authenticate or provide access to resources. A simple replication issue can keep an updated password from syncing to a remote DC, thus denying a logon request using the updated password. Understanding whether replication between any and all DCs is occurring and is up to date is necessary for the underlying health of AD.
- **SolarWinds Insights: Monitoring Replication**
  AD replication serves as the basis of ensuring all authentication—both on-prem and in the cloud—is correct and up to date. Without proper replication, all changes to AD impacting access to network resources remain outdated, potentially allowing continued access to accounts and/or resources. But monitoring replication is more than checking the current status; it involves both understanding whether the service is functioning, but also why if it's not.

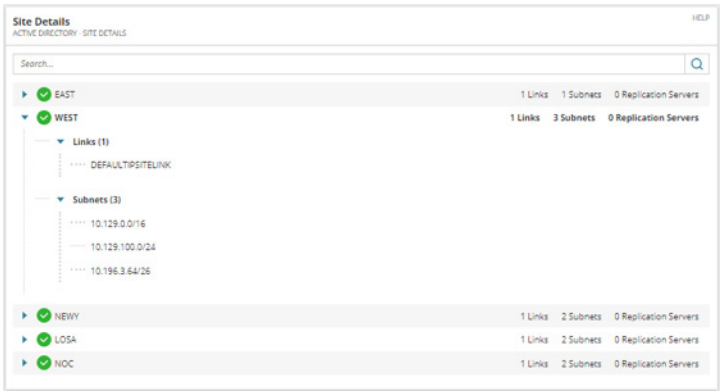
  Server & Application Monitor provides both replication status and detail information, giving IT teams complete visibility into not just whether replication is "good," but also what about it has failed and why.



- **Domain Controller Roles** – DCs taking on flexible single master operations (FSMO) roles need to be monitored to determine if foundational functions are working. Specific roles, such as the PDC Emulator, can impact users directly where password and group policy updates can fail without its presence.

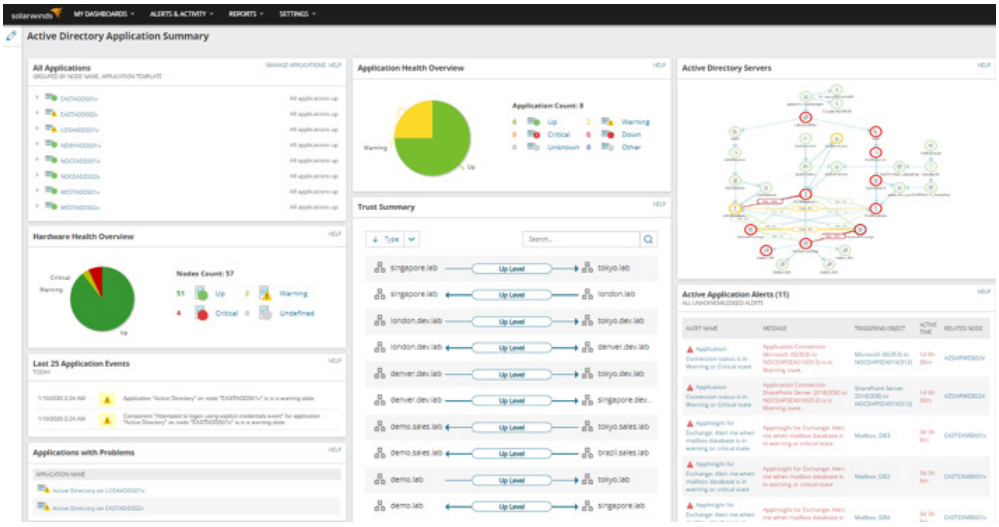


- **AD Sites** – Sites define the IP address subnets they host, and the links between sites used for replication. While they don't change often, making a simple change to an IP subnet can have ripple effects for AD-integrated services using Sites to also define how they communicate with AD.



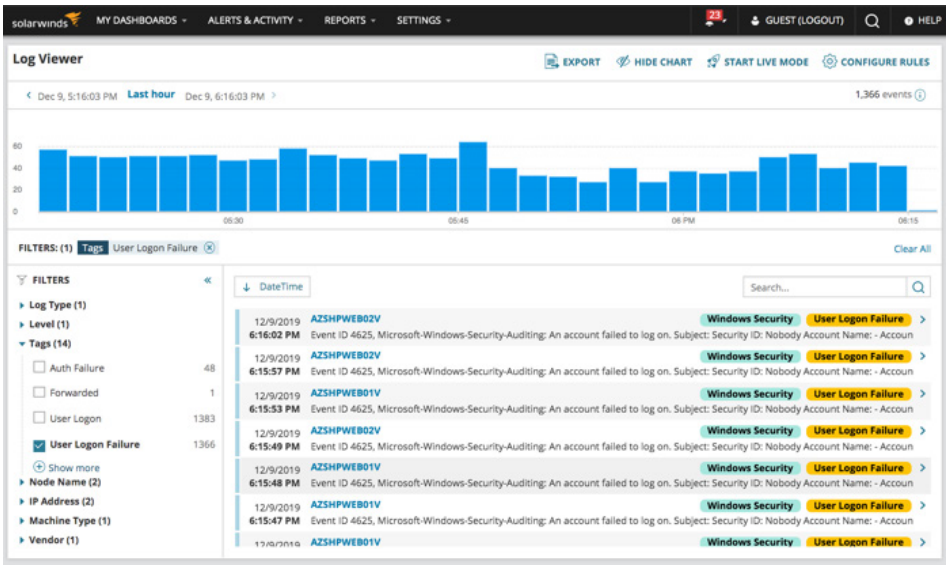
- **SolarWinds Insights: Seeing Active Directory From 10,000 Feet**
  Because the state of AD can be constantly changing, understanding the root cause of an issue is necessary to provide a timely response. So, purely relying on scanning logs and interpreting entries isn't going to be insightful.

  Server & Application Monitor provides a high-level view of AD (shown below), giving IT teams a window into the current state of AD. With an ability to drill down into nearly every facet of the dashboard, Server & Application Monitor makes it easy to quickly navigate to the aspect of AD in question, providing contextual details to help identify and remedy the issue.



- **Logons and Windows Events** – Lots of other events reflect changes within AD potentially having adverse effects on everything from an individual users' ability to log on to many users no longer being able to access resources due to group membership changes.

- **SolarWinds Insights: Taking Advantage of Logged Events**
  Vendors like Microsoft have made efforts to provide substantial amounts of detail in their event logs. Changes made to the configuration of AD which may not be obvious when looking at dashboards designed to look at the overall health of AD will still show up in the logs. So, it's important to consider taking advantage of all the log data provided to identify potentially suspicious, harmful, or otherwise unsanctioned actions potentially impacting AD.
  For example, Log Analyzer (shown below) can highlight user logon failures. When logged at abnormal timeframes, these failures can indicate an attempted logon by someone without proper access to the network.



Reason #3: A Secure AD Is a Healthy AD

AD is a prime target for cyberattacks. With 60% of all attacks leveraging lateral movement within your network[1], it's evident attackers need to compromise credentials giving them access to the systems, applications, and data they require to carry out their dastardly plans. So, AD need to be carefully monitored for any changes being made.

Additionally, newer compliance mandates are including specific requirements around putting security in place, knowing when security has been modified to impact data privacy, and an ability to remediate issues and return the environment to a known-compliant state. They're also including defined penalties should a breach occur due to the lack of a secure environment.

So, it's important to take steps to make your AD both secure and compliant. This partially requires a focus on monitoring specific types of changes within AD (e.g., modifications to group memberships, creation of multiple user accounts in a short period of time, etc.) and any actions taking upon specific objects (e.g., the Domain Admin's group, the Administrator account, etc.).

Additionally, there are a few best practices to help ensure AD remains secure:

- **Utilize Least Privilege** – when creating groups or assigning permissions, it's imperative you do so with the principle of least privilege in mind, where access is restricted to only those permissions needed. This helps to limit the threat surface of a cyberattack, and makes it more difficult for attackers to gain access to AD, systems, and data.

[1]Carbon Black, *Global Threat Report (2019)*

- **Limit AD Admin** – Attackers seeking to move laterally within your network are always looking for privileged accounts; especially those with admin rights to some or all of AD to create accounts and grant access via group memberships. Limiting the number of user accounts with access to the Domain Admins and Global Admins groups helps to restrict an attacker's ability to establish persistence and self-grant access.
- **Employ Auditing and Alerting** – There are so many leading and active indicators of threatening activity, there's no way a human can keep track of it all on their own. Enabling the auditing of logons and changes in AD gives you visibility into activity deemed suspicious or threatening. Alerting can be used to ensure timely response by IT or security teams should inappropriate activity occur.
- **SolarWinds Insights: Auditing AD Changes from the Event Log** Just about every change to your AD shows up one way or another into the Windows Event Logs. So, these logs provide you with pertinent details around changes to group memberships, account creations and deletions, and more—all of which can be malicious in intent. *Log Analyzer* can be used to centralize the collection, monitoring, and review of specific AD changes you deem inappropriate or suspicious.
- **Backup AD Regularly** – Should an attacker gain access to AD and make any changes, you need a way to recover AD back to a *known-secure* state prior to an attack.
- **Patch Vulnerabilities** – This goes for domain controllers and every other system. Every day, attacks leverage vulnerabilities in operating systems, applications, and browsers. Making certain these are all up to date on patches helps to minimize the threat surface in AD.

Remember, AD Needs Monitoring

AD management has become a routine task for most IT organizations, so the idea of monitoring it to make sure it's running, meeting performance expectations, and is secure, has become "the forgotten necessity."

But, with AD being *the* most critical service on your network, it's imperative you include one or more of the elements covered in this whitepaper. The goal is to make sure AD—and the underlying hardware, operating systems, and services making it function—all are running within acceptable levels. And if they shouldn't be, IT should be have an ability to quickly gain contextual insight into both what's wrong and why.

It's likely most of you reading this have forgotten the need to include AD as part of your "critical workload" monitoring. But, given AD's importance, many parts of it need to be watched on a daily basis to ensure its performance and security both today and in the future.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-prem, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx