Domain Report

Microsoft Active Directory is the core of your network infrastructure just like the foundation of your house. If your foundation has cracks, it will affect your entire business structure. From slow log-ons and network hassles to security holes and migration problems; Active Directory if not organized properly can be a huge obstacle to the successful momentum and growth of any company.

Without a high level of expertise, it is very difficult to track down the cracks in any Active Directory architecture. It takes time to scan the domain, find the problems, the reach of their impact, and consider the potential consequence of every change made. Doing this without knowing exactly where to look and what the effect will be, is very risky and will cost many hours in research alone.

Synchronis-IT has over 20 years' experience hunting down AD problems and fixing them. We know what to look for, what changes should be made and what the impact will be for each adjustment. This report is a compilation of the issues our team discovered with the Starsys Medical architecture. It is our recommendation that repairs and adjustments be made.

Domain Report

During an Active Directory Health Check, it's not uncommon to uncover a wide range of issues. The threat factor can range from catastrophic to negligible, and the time window can range from immediate to six-months away. We have developed a simple severity guide to assist with assessing the threat factor. Our system contains four separate severity ratings, starting with Critical Severity, High Severity, Medium Severity, and the final category, Warning Severity. Any given environment can contain issues that fall into every category, or even issues that span all categories at once.

It's generally recommended that CRTICAL issues are addressed almost immediately. HIGH Severity issues should be addressed in short order, usually quickly after CRTICIAL issues. Medium Severity should be solved within a few weeks of addressing threats in the Environment. Warning issues can range from immediate to a few months in the priority they should be fixed.

It is important to note, that while these guidelines are meant to help prioritize the risks, every issue represents a risk for damage, failure, or total loss in the environment. While some threats are minor, it is also entirely possible for a minor threat to become a major threat at any time. It is recommended that all issues be resolved to ensure smooth day to day operation and prevent any loss to the Starsys Medical network environment and critical systems.

Critical Issues should be corrected as soon as possible, unless other steps have been taken to mitigate loss.

High Severity are urgent issues that could become critical if not addressed. Loss is likely to occur.

Medium Severity issues are interfering with basic system Functions and services, and could become critical the longer left unaddressed.

Warning Issues have a low impact on overall System Health, but a greater impact on a single service.

CRITICAL

Failure of Backup Systems

In the Domain, the backup systems are not functioning properly. The last successful Active Directive Backup was executed for servers STARSYS-2, STARSYS-1 and STARSYS-3 on July 11th, 2017 (07/11/2017). Not only is the backup over 3 months old, but it is also 30 days older than the tombstone life active on the Domain.

A tombstone lifetime represents the period of time during which a deleted AD object can be recovered, with a currently configured lifetime of 60 days. According to Microsoft, a backup older than the tombstone lifetime is not a good backup. Active Directory uses this tombstone lifetime in the backup and restore process to protect against inconsistent data.

Incomplete Migration

There is evidence to support that the migration from 2008 to 2012 was not completed in its entirety. Additionally, the migration from starsysmed to starsysmed.local is also incomplete.

Inconsistency in DNS Servers

Active Directory comes with a host of load balancing and fail-safe options. The Environment are being plagued by inconsistency in both naming and configuration of DNS Servers. Each DNS Server is configured differently.

Untrusted Domain in AD Forest

In Active Directory, trusts are relationships between domains to allow authentication in which a trusting domain honors the logon authentications of a trusted domain. In the Forest, where a second Domain exists or is referenced, only starsysmed.local is trusted. Even with starsysmed.local directing to starsysmed, it is still untrusted, leading to a denial or slowdown of authentications.

CRITICAL—SECURITY

Enterprise Administrators are present

Following Microsoft Best Practice and assuming standard Security Rules, it is highly recommended there are no Enterprise Administrators. Most administrative work can be done with a Domain Administrator account. The Enterprise Admins group, which is housed in the forest root domain, should contain no users on a day-to-day basis.

Auditing should be configured to send alerts if any modifications are made to the properties or membership of the EA group. These alerts should be sent, at a minimum, to users or teams responsible for Active Directory administration and incident response.

Microsoft's stance:

"Most security-related training courses and documentation discuss the implementation of a principle of least privilege, yet organizations rarely follow it. The principle is simple, and the impact of applying it correctly greatly increases your security and reduces your risk. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers."

Windows updates

In the STARSYS-2 server, the Windows Update Service has never been configured or executed, making patches out of date and the server extremely vulnerable to attacks.

Updates for the STARSYS-3 server were last installed in 2016.

The STARSYS-1 server is actively attempting to patch and stay up to date with Windows Update Service, but is failing the installation for a majority of updates.

A proper Windows update would resolve a large variety of issues. The Windows updates would serve to protect against malicious software by the constant addition of critical security patches. They will also resolve general bugs within Windows and Windows Server.

HIGH SEVERITY—AD MANAGEABILITY

Global Catalogue Error

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in an Active Directory Domain Services (AD DS) forest. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

The Global Catalogue references starsysmed.local, while both sites and DNS records often point to starsysmed. This gives evidence of the second existing domain, and contributes to starsysmed being untrusted.

Domain Controller Inconsistency

Each Domain Controller points to different DNS servers. Some point to starsysmed.local and others just to starsys.med for DNS resolution, leading to dead-end DNS request and over all slow down.

It should be noted that Microsoft says, “For example, Domain Name System (DNS) problems, networking issues, or security problems can all cause Active Directory replication to fail.”

Certification Services

Certification Services, a key component, is offline for the STARSYS-3 server.

Active Directory Certificate Services (AD CS) provides customizable services for Issuing and managing certificates in software security systems that use public key technologies.

HIGH SEVERITY—AD MANAGEABILITY

Printer Policy Bloat

All three Active Directory servers suffer significant slowdown when applying Printer Group Policy. There was evidence of printer driver errors, and missing scripts in the group policy.

Inheritance Blocking

Group Policy uses Inheritance Blocking along with Default Group Policy Objects. Organizational Units are used to group objects, including accounts and resources in a domain, for administrative purposes, such as the application of Group Policy or delegation of authority. Using Default GPO's instead, creates unnecessary settings and bloat in Group Policy. A clean up and restructure is highly recommended.

Domain Controller Inconsistency

Certification errors exist on all servers, this is causing Certification Authority to not work properly. The Certification Authority is primary tool for managing a certificate, certificate revocation, and certificate enrollment. This service helps with managing enrollment and revocation of certificates for users, computers, services, and network devices such as routers

MEDIUM SEVERITY—REPLICATION

STARSYS-1 Replication

The STARSYS-1 Server has a 33% Failure Rate, failing 5 of 15 attempts to replicate to the STARSYS-3 and STARSYS-2 servers. According to Microsoft, Active Directory replication problems can have several different sources. Domain Name System (DNS) problems, networking issues, or security problems can all cause Active Directory replication to fail.

The physical domain controller contains the domain partition data that is replicated to other domain controllers in that same domain.

Within the scope of a forest, sites are a representation of the physical network topology. This includes users, computers, physical subnet and site definitions. Replication of updates to domain data occurs between multiple domain controllers to keep replicas synchronized.

MEDIUM SEVERITY—SECURITY

Built-in administrator is active

Built-In Administrators are also Enterprise Administrators. This represents a significant risk.

Microsoft best practice being the following:

If the Administrator account is not already disabled, disable it when you have completed configuration of the account's properties. This prevents the account from being used for any purpose unless it is first enabled. In a disaster recovery scenario in which no accounts are available to perform repairs of the AD DS environment, you can boot a domain controller into safe mode, log on locally with the built-in Administrator account

Non-expiring passwords

109 Accounts have passwords that have not been changed in the last 90 days. These rules can be changed, based on your Organization's security goals, they do represent a significant risk.

If the Maximum password age policy setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization because users might keep their passwords in an unsecured location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

Outdated Server Software

The installed operating system on the Domain Controller is out of date. The servers are currently running Windows 2012 R2. It is recommended to migrate the environment to Microsoft Windows Server 2016 edition.

WARNINGS

WINS

WINS is running and active, but not configured. This represents a security risk as it was retired over 15 years ago in favor of DNS. This is an outdated service.

Microsoft has an official response from this year:

In June of 2017, Microsoft replied […], saying, "a fix would require a complete overhaul of the code to be considered comprehensive. The functionality provided by WINS was replaced by DNS and Microsoft has advised customers to migrate away from it." That is, Microsoft will not be patching this vulnerability due to the amount of work that would be required. Instead, Microsoft is recommending that users replace WINS with DNS.

STARSYS-3 LOW HARD DISK

The STARSYS-3 server is low on physical disk space. Low disk space increases file fragmentation, which can affect server performance if fragmented files are accessed. This decreases performance of the whole VMware cluster.

DNS PRIORITY ERRORS

Each Active Directory server points to the other DNS servers, while listing themselves as the last server at the same time. This leads to each server asking other servers to perform name resolution before checking their own records.

It is recommended to change the priority.

REFERENCES

Billmath. "Implementing Least-Privilege Administrative Models."

Microsoft Docs,

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

"Maximum password age."

Windows Server,

https://technet.microsoft.com/en-us/library/hh994573(v=ws.11).aspx

"WINS Server Remote Memory Corruption Vulnerability in Microsoft Windows Server."

Fortinet Blog, 14 June 2017,

https://blog.fortinet.com/2017/06/14/wins-server-remote-memory-corruption-vulnerability-in-microsoft-windows-server

"Troubleshooting Active Directory Replication Problems."

Windows Server,

https://technet.microsoft.com/en-us/library/cc949120(v=ws.10).aspx