Active Directory Best Practices

Nasuni Corporation – Boston, MA

Overview

The following are best practices when installing the Nasuni Filer into an Active Directory environment.

Use lower-case hostnames

When specifying a hostname, use lower-case letters.

Use a Fully Qualified Domain Name (FQDN)

When joining a Nasuni Filer to an Active Directory domain, the Nasuni Filer should have a fully qualified domain name (FQDN) that matches the Active Directory domain. Otherwise, clients might have trouble discovering the Nasuni Filer by name.

Only one DNS “A” record for each Nasuni Filer

There should only be one DNS “A” record for each Nasuni Filer.

Additional names for Nasuni Filer

To specify additional names for a Nasuni Filer, add CNAME records to the DNS entry.

Forward and Reverse DNS for all Nasuni Filers

Each Nasuni Filer should have PTR records that are consistent for both forward and reverse DNS. If forward/reverse resolution is not consistent, clients might have issues authenticating to the Nasuni Filer.

Matching hostname

The A record, the PTR record, and the hostname must all be exactly the same.

Ensure "Sites and Services" in Active Directory is configured correctly

Active Directory “Sites and Services” is a Microsoft Management Console (MMC) snap-in that you can use to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest. This snap-in also provides a view of the service-specific objects that are published in AD DS.

If the Active Directory “Sites and Services” feature is not configured correctly, the Nasuni Filer might not contact the correct domain controller when authenticating.

Ensure that the IP addresses of the Nasuni Filer and the NMC are added to the Active Directory “Sites and Services” subnet object on which the Nasuni Filer resides.

Prefer Active Directory domain controller for NTP when available

For Kerberos to work correctly, the Nasuni Filer and the domain controller must have the same time. If the times are different, Kerberos stops authenticating. Therefore, if the Active Directory domain controller is configured to serve Network Time Protocol (NTP) requests, prefer using NTP services from the Active Directory domain controller. This ensures the proper time synchronization needed for Kerberos.

Nasuni recommends that you use the Nasuni Filer’s "Filer Time Configuration" page to set the Time Server to 1 - 4 of the closest Active Directory domain controllers to use as Time Servers, if that information is available.

If that information is not available, you can try using “NTP from Domain Controllers” when joining the Nasuni Filer to the Active Directory domain. However, the latter configuration is not aware of sites and services, and you might experience performance issues.

If no NTP services are available from domain controllers, the current NTP server is used.

DNS TXT record for Kerberos

A `_kerberos` TXT record for Kerberos is required in DNS, such as the following:

```
_kerberos.example.com  TXT  "example.com"
```

where `example.com` is the Active Directory domain that the Nasuni Filer is joined to.

Has the patch "Security Update for SAM and LSAD Remote Protocols (3148527)" (https://technet.microsoft.com/en-us/library/security/ms16-047.aspx) been installed?

After applying this patch, it might become necessary for the Nasuni Filer to rejoin the Active Directory domain.

Questions?

If you have any questions about Active Directory best practices, please contact Nasuni Technical Support.