


# Why using .local as your domain name extension is a BAD idea!

 [community.veeam.com/blogs-and-podcasts-57/why-using-local-as-your-domain-name-extension-is-a-bad-idea-4828](https://community.veeam.com/blogs-and-podcasts-57/why-using-local-as-your-domain-name-extension-is-a-bad-idea-4828)

Viperian



- [Viperian](#)
- Product Strategy
- 24 comments

The special-purpose .local top-level domain (TLD) is not designed for use in the global Domain Name System (DNS). Rather, multicast DNS (mDNS) uses it to resolve hostnames to IP addresses within small networks, eliminating the need for a dedicated DNS server. Specifically, mDNS operates on the local network link and uses the .local TLD for this purpose. When an mDNS client needs to resolve a hostname that ends with .local, it sends queries to the mDNS IPv4 link-local multicast address 224.0.0.251 or its IPv6 equivalent ff02::fb.

## Top 5 reasons why it is a bad idea

Let's dive into why using the .local top-level domain (TLD) can lead to a handful of issues.

1. **Standards Compliance:** The Internet Engineering Task Force (IETF) reserves the .local TLD for mDNS in RFC 6762. If you use it in another context or within a traditional unicast DNS context, you may face non-compliant behavior and conflicts.
2. **Compatibility Issues:** Systems, particularly those running Apple's Bonjour service, frequently use mDNS and expect the .local TLD to behave a certain way. Non-standard use of .local can cause compatibility issues.
3. **Potential for Naming Conflicts:** Any .local domain is up for grabs for devices using mDNS. If a device using mDNS and a device on your network both claim the same .local domain, you've got a naming conflict on your hands.
4. **Not Globally Unique or Routable:** Global DNS doesn't recognize .local domains, and they aren't globally unique. So, they're unfit for services that need to access outside your local network. While this isn't typically an issue for internal domains, it can become one when you need to connect services to the outside world.
5. **Potential for Future Conflicts:** Although .local is currently reserved for mDNS, it could potentially conflict with future internet standards or practices if you use it in a non-compliant way.

## Linux and .local as domain extension are NO friends

If you're thinking of using .local domains and mDNS in a Linux server environment, you might want to rethink that. It can introduce several issues, particularly if your network includes other devices and systems that interact with mDNS and DNS. Here are the top five potential problems:

1. **Naming Conflicts:** Devices using mDNS can claim any .local domain automatically, so you might have naming conflicts if a Linux server uses a .local domain for unicast DNS and a device attempts to claim the same name via mDNS.
2. **Service Discovery Issues:** mDNS is typically used for service discovery in local networks. Using .local domains in a traditional DNS context might interfere with mDNS service discovery, leading to incorrect or failed service discovery.
3. **Incompatibility with Avahi/Bonjour:** Linux uses the Avahi daemon for mDNS, while Apple devices use Bonjour. Using .local domains for traditional DNS might cause compatibility issues with Avahi, Bonjour, and other systems expecting .local to be used with mDNS.
4. **Resolution Delays or Failures:** Depending on your network configuration and the specific systems and software you're using, DNS resolution for .local domains may be slow or might fail completely.
5. **Difficulty in Troubleshooting:** Because using .local in a traditional DNS context isn't standard, troubleshooting network issues might become more challenging.

So, while you can use .local domains and mDNS in a Linux server environment, it's generally better to use a valid registered domain name to avoid these potential issues.

## Troubleshooting potential .local TLD domain causing issues

---

If you suspect your .local domain is causing problems in your personal network, here are a few steps for diagnosis:

1. **Check for Naming Conflicts:** First, check for naming conflicts in your network using tools like avahi-browse (on Linux) or dns-sd (on macOS) to see what .local names are in use on your network.

On Linux, you can use Avahi to browse services with:

```
avahi-browse -all
```

On macOS, you can use dns-sd:

```
dns-sd -B _services._dns-sd._udp
```

2. **Try Manual Resolution:** Attempt to manually resolve the .local domain names in question using the ping command.
3. **Check Logs:** Review the system logs on your server and other devices for any error messages or warnings related to DNS resolution or mDNS.
4. **Test Different Devices:** Try accessing the .local domain from different devices on your network to see if some devices can access it while others can't.

5. **Disable and Enable mDNS:** Try temporarily disabling mDNS on Linux through Avahi and check if the problem continues. If disabling mDNS resolves the issue, it strongly suggests a connection to your .local domain.
6. **Use Network Troubleshooting Tools:** You can use tools like dig, nslookup, and traceroute to get more information about the potential points of failure in DNS resolution. Additionally, Wireshark, a network protocol analyzer, can assist by displaying mDNS packets along with DNS requests and responses on the network.

## Conclusion

---

Keep in mind, mDNS reserves the .local TLD, and it's not a standard practice to use it in other contexts. If you're dealing with ongoing issues, think about modifying your DNS setup to use a different TLD or a subdomain of a domain under your control.

These replacements for .local often come into play:

- .lan
- .private
- .internal
- .corp
- .home
- .network
- .intranet
- .site

However, the best practice remains to use a subdomain of a domain you own. For instance, if you own **mydomain.com**, consider using **internal.mydomain.com** for your internal network. This approach ensures you align with standard practices and avoids potential issues with future TLDs or conflicts with mDNS or other services.

## 24 comments

---



+11

- [lams3le](#)
- Veeam Legend
- 1352 comments
- 1 year ago

This is great [@Viperian](#)! Thank you for sharing. This issue will be evident when you are even synchronising an on-premise AD environment with the .local extension with Azure AD. Microsoft strongly recommends that you **register a public domain and use subdomains for the internal DNS** as you have mentioned in the concluding part of your article.

To me, the only advantage of using .local as a domain extension is that it cannot be routed over the internet.

---



+22

- [MicoolPaul](#)
- 2343 comments
- 1 year ago

Hi [@Viperian](#)!

This was a great read, thank you for sharing 😊

I found it particularly interesting because I've been advocating to not use non-routable TLDs for a while, but never because of the mDNS reason you mentioned, I learned about it from reading this post.

I used to do a lot with PKI, and one of the key demands for a sub-domain on a public domain was because in 2016 the trusted certificate authorities agreed to revoke any SSL certificates signed to IP addresses or "intranet names" such as server1.local

I find it shocking on reflection that it was once allowed, but times can certainly change things!

---



+11

- [wolff.mateus](#)
- Veeam Vanguard
- 526 comments
- 1 year ago

Nice post [@Viperian](#)!

---



+20

- [coolsport00](#)
- Veeam Legend
- 3965 comments
- 1 year ago

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

---



+22

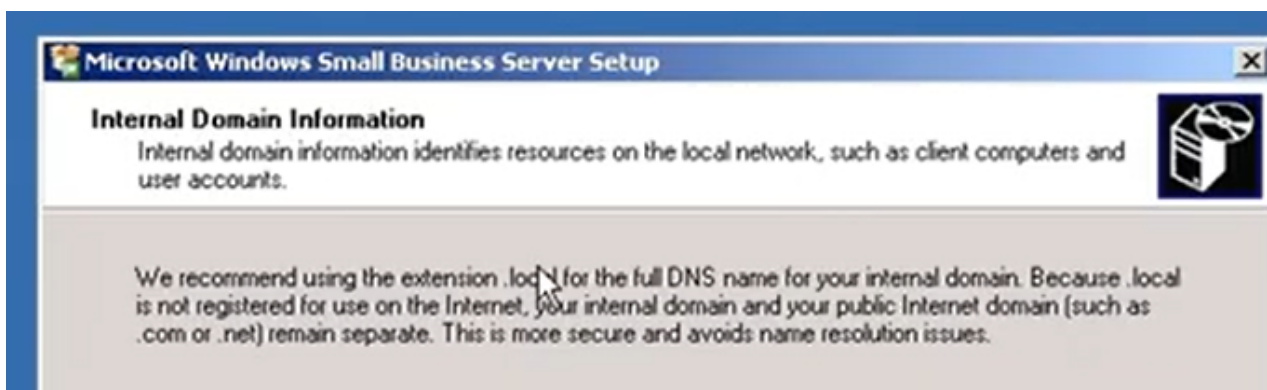
- [MicoolPaul](#)
- 2343 comments
- 1 year ago

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Absolutely, once upon a time Microsoft recommended it.

I remember SBS 2003 strongly advocating for it, so I dug out the installer screen:



Alt Text: "We recommend using the extension .local for the full DNS name for your internal domain. Because .local is not registered for use on the Internet, your internal domain and your public Internet domain (such as .com or .net) remain separate. This is more secure and avoids name resolution issues."

---



+20

- [coolsport00](#)
- Veeam Legend
- 3965 comments
- 1 year ago

hahaha GREAT find [@MicoolPaul](#) !! 😊

---



+11

- [iams3le](#)
- Veeam Legend
- 1352 comments
- 1 year ago

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

> back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Exactly!



+11

- [iams3le](#)
- Veeam Legend
- 1352 comments
- 1 year ago

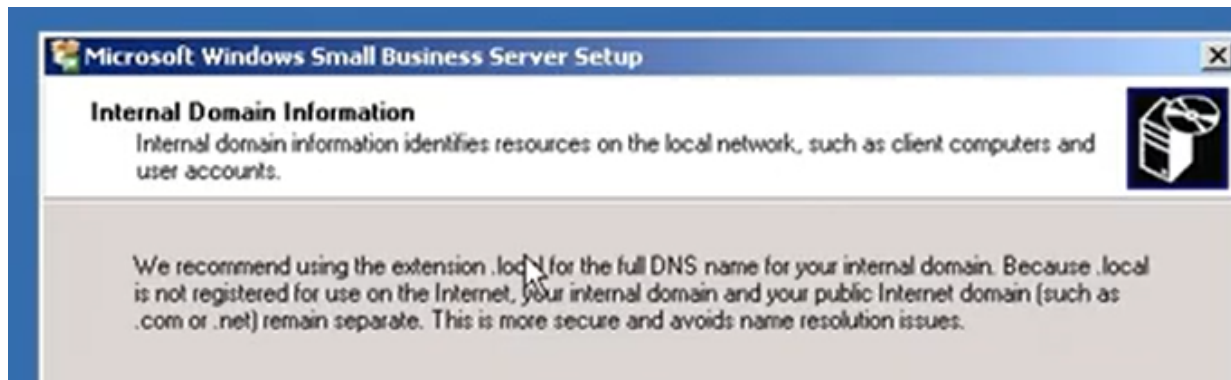
MicoolPaul wrote:

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Absolutely, once upon a time Microsoft recommended it.

I remember SBS 2003 strongly advocating for it, so I dug out the installer screen:



Alt Text: "We recommend using the extension .local for the full DNS name for your internal domain. Because .local is not registered for use on the Internet, your internal domain and your public Internet domain (such as .com or .net) remain separate. This is more secure and avoids name resolution issues."

At this point, they were myopic and never envisaged the rapid influx of technologies... The only constant in Life is change tho!

---



+21

- [Chris.Childerhose](#)
- Veeam Legend, Veeam Vanguard
- 8115 comments
- 1 year ago

Interesting read and thanks for sharing. I actually use .lab for home.

---



+11

- [lams3le](#)
- Veeam Legend
- 1352 comments
- 1 year ago

Chris.Childerhose wrote:

Interesting read and thanks for sharing. I actually use .lab for home.

I still do. But here is a [blogpost](#) of how i fixed the issue you might encounter when syncing with Azure AD.

---





+21

- [Chris.Childerhose](#)
- Veeam Legend, Veeam Vanguard
- 8115 comments
- 1 year ago

lams3le wrote:

Chris.Childerhose wrote:

Interesting read and thanks for sharing. I actually use .lab for home.

I still do. But here is a [blogpost](#) of how i fixed the issue you might encounter when syncing with Azure AD.

That is a really great article, thanks for sharing that. 👍

---



+10

- [Link State](#)
- Veeam Legend
- 577 comments
- 1 year ago

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

MicoolPaul wrote:

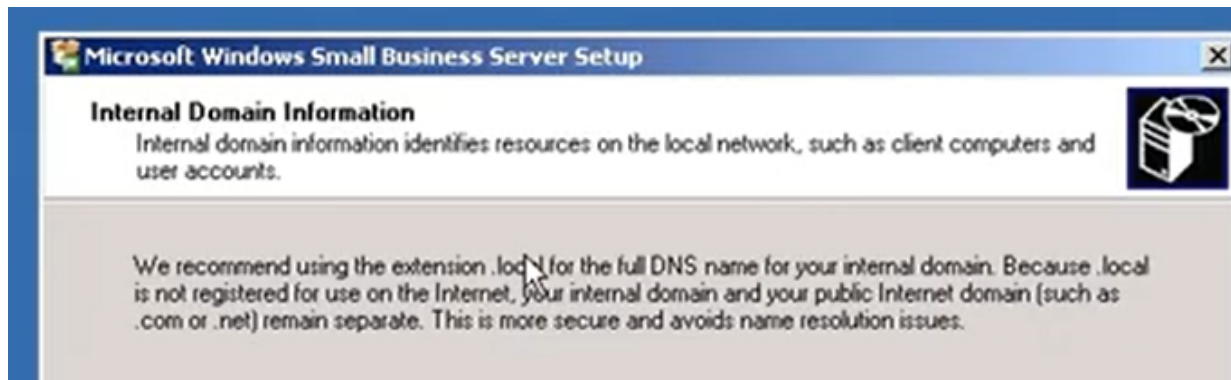
coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Absolutely, once upon a time Microsoft recommended it.

I remember SBS 2003 strongly advocating for it, so I dug out the installer screen:





Alt Text: "We recommend using the extension .local for the full DNS name for your internal domain. Because .local is not registered for use on the Internet, your internal domain and your public Internet domain (such as .com or .net) remain separate. This is more secure and avoids name resolution issues."

If I remember correctly in the DC 2003 setup they recommended using .local to avoid DNS splitbrain.

So as not to have an intranet and pub domain with identical fqdn.



+7

- [Viperian](#)
- Author
- Product Strategy
- 24 comments
- 1 year ago

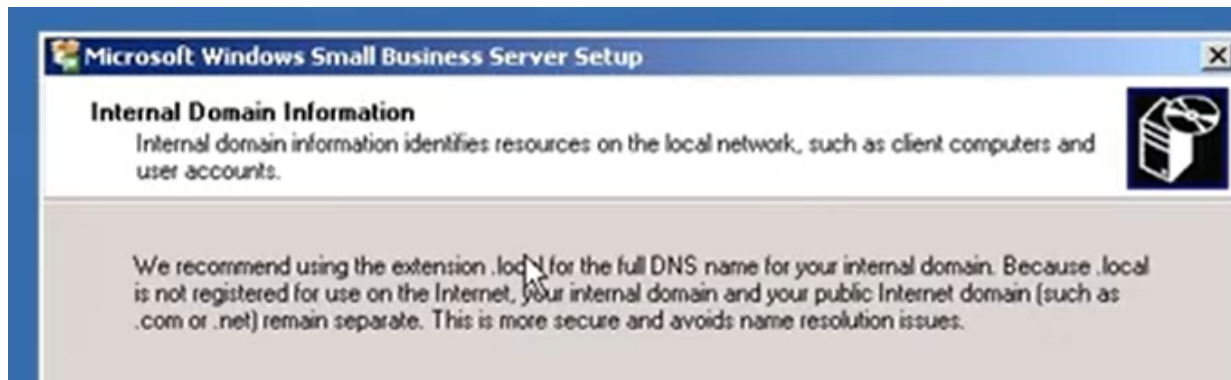
MicoolPaul wrote:

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Absolutely, once upon a time Microsoft recommended it.

I remember SBS 2003 strongly advocating for it, so I dug out the installer screen:



Alt Text: "We recommend using the extension .local for the full DNS name for your internal domain. Because .local is not registered for use on the Internet, your internal domain and your public Internet domain (such as .com or .net) remain separate. This is more secure and avoids name resolution issues."

The ".local" domain in DNS officially became a no-go in 2013. This was when it was formally specified for use in private networks as part of something called the Zero Configuration Networking (Zeroconf) standards, which also includes a protocol known as Multicast DNS.

Before then, some organizations were actually using ".local" as part of their internal domain name setup for Active Directory, based on Microsoft's advice. But, once ".local" was reserved for private networks and wasn't recognized as a legitimate top-level domain by the folks that oversee these things (the Internet Assigned Numbers Authority), it started causing all sorts of problems with domain name resolution.

So, Microsoft changed its tune and now recommends using a subdomain of a domain that you actually own for your internal Active Directory names. That, or you can use a domain that's reserved for testing and documentation purposes. Long story short, using ".local" in a global DNS context? Not a great idea.



+14

- [regnor](#)
- Veeam MVP
- 1333 comments
- 1 year ago

Just like [@lams3le](#), I often see .local as an issue when doing AAD Connect and migrations to Exchange Online. In the worst case .local is used as an internal email domain, so you need to change different systems and workflows.





+5

- [MarcoLuvisi](#)
- Influencer
- 228 comments
- 1 year ago

Viperian wrote:

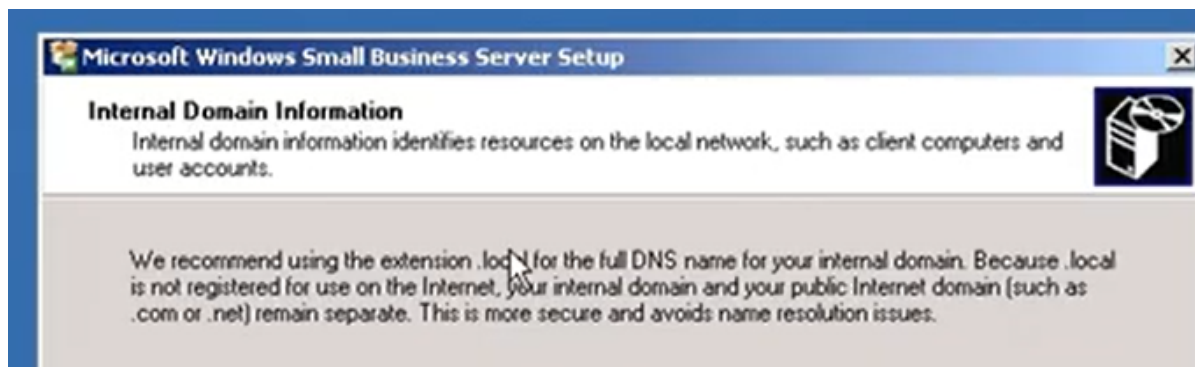
MicoolPaul wrote:

coolsport00 wrote:

Interesting read. Thank you for posting [@Viperian](#) . A lot of info I wasn't aware of. Funny how tech changes sometimes...back in the early AD days how .local was "suggested" for use, at least in the arenas I was around. Good stuff!

Absolutely, once upon a time Microsoft recommended it.

I remember SBS 2003 strongly advocating for it, so I dug out the installer screen:



Alt Text: "We recommend using the extension .local for the full DNS name for your internal domain. Because .local is not registered for use on the Internet, your internal domain and your public Internet domain (such as .com or .net) remain separate. This is more secure and avoids name resolution issues."

The ".local" domain in DNS officially became a no-go in 2013. This was when it was formally specified for use in private networks as part of something called the Zero Configuration Networking (Zeroconf) standards, which also includes a protocol known as Multicast DNS.

Before then, some organizations were actually using ".local" as part of their internal domain name setup for Active Directory, based on Microsoft's advice. But, once ".local" was reserved for private networks and wasn't recognized as a legitimate top-level domain by the folks that oversee these things (the Internet Assigned Numbers Authority), it started causing all sorts of problems with domain name resolution.

So, Microsoft changed its tune and now recommends using a subdomain of a domain that you actually own for your internal Active Directory names. That, or you can use a domain that's reserved for testing and documentation purposes. Long story short, using ".local" in

a global DNS context? Not a great idea.

Great analysis [@Viperian](#) !

---



 +6

- [dloseke](#)
- Veeam Legend
- 1426 comments
- 1 year ago

Chris.Childerhose wrote:

Interesting read and thanks for sharing. I actually use .lab for home.

My home lab is root.local, but my lab at work is ad.proofinc.com. Unfortunately, proofinc.com does exist, so I do get some weird DNS resolution at times. Any time I create a new domain, it's going to ad.domain.com or corp.domain.com. Obviously, not great to just use domain.com when it matches your website domain, but one of my counterparts recently spun one of these up and we did get some of the same DNS resolution issues expected, but we at least have the know workarounds.

---



 +8

- [HunterLAFR](#)
- Veeam Legend
- 420 comments
- 1 year ago

Nice info,

I normally use for the lab .lab

and for prod, it was a time we used .local, but with the massive use of internet, and tons of applications published and internal and external use, at the end, we started using our .com domain locally and externally.

that WS2003 bring me a lot of memories.... what a days....

cheers!

---



- [williamdes](#)

- New Here
- 1 comment
- 1 year ago

You did suggest this list of TLDs, but two of them should never be used !

This is the checklist:

- .lan → RFC 6762 Appendix G
  - .private → RFC 6762 Appendix G
  - .internal → RFC 6762 Appendix G
  - .corp → RFC 6762 Appendix G
  - .home → RFC 6762 Appendix G
  - .network → NOT OKAY → I have a real domain: datacenters.network
  - .intranet → RFC 6762 Appendix G
  - .site → NOT OKAY → also a real  
TLD: <https://www.ovhcloud.com/fr/domains/tld/site/> (random example: ovh.site)
- 

## B

- BackupBytesTim
- Comes here often
- 17 comments
- 1 year ago

Good tips for sure, also worth noting though it's important when using a publicly available name, to own it. I had a customer once who used a domain name ("badidea.com" for explanatory reasons) that they didn't own. Another company owned it and had it registered so public DNS records pointed somewhere else. It caused new problems seemingly every week because every computer was always trying to contact badidea.com over the internet to someone else's servers to reach the domain and so things were always broken. It took two years as their MSP to convince them to change to something they owned.

So my advice is firstly, if you are NOT using .local, definitely, always, every time, own the domain, they're not that expensive.

---



 +6

- dloseke
- Veeam Legend
- 1426 comments
- 1 year ago

BackupBytesTim wrote:

Good tips for sure, also worth noting though it's important when using a publicly available name, to own it. I had a customer once who used a domain name ("badidea.com" for explanatory reasons) that they didn't own. Another company owned it and had it registered so public DNS records pointed somewhere else. It caused new problems seemingly every week because every computer was always trying to contact badidea.com over the internet to someone else's servers to reach the domain and so things were always broken. It took two years as their MSP to convince them to change to something they owned.

So my advice is firstly, if you are NOT using .local, definitely, always, every time, own the domain, they're not that expensive.

You raise a good point. My lab environment utilizes a subdomain where I don't own the parent domain. It works in theory, but I have certainly had instances where things do try and connect to the parent domain. For a lab, maybe not a big deal, but if this was a production environment, this would be terrible!