Global Samba 4 AD Domain Tips and Tricks

Disclaimer

This presentation, the content and opinions contained within are the authors' own and do not reflect the views or opinions of Indeed, Inc.

Last year's presentation

- Audio: https://sambaxp.org/archive_data/SambaXP2017-AUDIO/Day3/Is%20Samba%204%20AD%20ready%20for%20Global%20Enterprise.mp3
- Slides: https://sambaxp.org/archive_data/SambaXP2017-SLIDES/Day3/Is%20Samba%204%20AD%20Ready%20for%20Global%20Enterprise%20-%20Kevin%20Kunkel.pdf

Kevin Kunkel

IT Systems, Indeed Inc.

About me (Kevin Kunkel)

- Windows 95 converted me to Linux
- Software Engineering at RIT, BS CS from Mercy College
- 12 years of Systems Administration
  - Linux SysAdmin
  - Windows SysAdmin
  - B2B SMB consulting
- 4 years managing large scale Samba AD

Carlos Gonzalez

IT Systems, Indeed Inc.

About Carlos

- Use to be a Mac SysAdmin
- Joined Indeed 2 years ago
- Now manages Indeed’s Samba AD Domain

But really, how about you?

This is for you.

You

- Samba Team
- Samba Developers
- Samba Users
- Enterprises/organizations/governments willing to try Samba

The past year for Samba AD

CVE-2018-1057

Password reset exploitation

- All passwords for all users had been susceptible to a bug that would allow anyone to change another user's password, since… FOREVER
  - **This is Bad**

Password reset exploitation

- All passwords for all users had been susceptible to a bug that would allow anyone to change another user's password, since… FOREVER
  - **This is Bad**
- Unless logging is set to 10 (full debug) this exploit would not generate any logs and be undetected. (possibly not even)
  - **This is Even Worse**

Actual impact?

- Truly very little. We have no evidence that this was ever exploited
- but
  - Reinforces a misperception that Samba isn't "enterprise-grade"
- **This is The Worst**

The patches

- Patches were dropped at 8am CEST
  - Great for Europe, Asia, Australia, Pacific Islands
  - Horrible time for the Americas (2am CDT for example)
- I'd like to propose a set time of day for important security updates.
- 2pm CEST - Midnight in New Zealand and 5am PDT
  - Fewest possible SysAd sleeping 1am-5am

Samba Bugs #13095 #13328 etc

Linked attribute mishandling/corruption

- Linked attributes have been the bane of Samba AD administrators
- I have too many repressed memories to elaborate on the causes

Theoretical Company

- Acme Global Corp is a large global multinational with over 10,000 employees, contractors and vendors.
- It has 10s of thousands of user objects in AD with 10s of thousands of groups objects.
- Many of these groups are used to facilitate RBAC to gate access to corporate networks and resources

Theoretical Impact

- Acme Global Corp has an “employees” group with over 7,000 members
- As a large multinational, employees come and go every day.

Before:

Alice
Bob
Charlie
...
Xavier

After:

Alice
Bob
Bob
...
Bob

Theoretical Impact (continued)

- Large swathes of users “removed” from “large” groups
- These same “large” groups are often used to gate access to standard applications and tools (think employees vs contractors vs vendors)
- Some SAML providers will sync AD membership and provision/delete application’s user accounts.
- Acme Global would have experienced widespread outages to core applications

Don’t put all your eggs in one basket!


IT is TOO RISKY

So what then?

- Can we have a single source of truth with multiple baskets?

No! Put all your eggs in one basket
AND THEN WATCH THAT BASKET!
- Andrew Carnegie

Monitoring

Nagios

- Port checks, both local and remotely
  - DNS: 53/tcp 53/udp 5353/tcp 5353/udp
  - Kerberos: 88/tcp 88/udp 464/tcp 464/udp
  - NTP 123/udp
  - SMB/CIFS: 135/tcp 135/udp 139/tcp 445/tcp
  - NETBIOS: 137/udp 138/udp
  - CIFS: 139/tcp
  - LDAP: 389/tcp 389/udp 636/tcp
  - Global Catalogue: 3268/tcp 3269/tcp
  - Dynamic RPC: 1024/tcp **OR** 49152/tcp

Nagios

- Local: **/usr/bin/sudo fuser 1024/tcp || /usr/bin/sudo fuser 49152/tcp**
- Remote: **echo test > /dev/tcp/$HOST_IP/1024 || echo test > /dev/tcp/$HOST_IP/49152**
- Samba-tool drs showrepl with some awk:

Nagios (check_drs_repl)

```
#!/bin/bash
sudo samba-tool drs showrepl -kno|awk '
BEGIN {
        FS="\t"; RS="" #Tab field separator, blankline record separator
#($1)DC=SAMDOM,DC=EXAMPLE,DC=COM
#       ($3)SITENAME\DOMAIN-CONTROLLER via RPC
#               ($6)DSA object GUID: 8974495f-a191-4d8b-84d1-25ff54f0d45a
#               ($9)Last attempt @ Mon May 30 12:14:32 2016 EDT was successful
#               ($12)0 consecutive failure(s).
#               ($15)Last success @ Mon May 30 12:14:32 2016 EDT
#

} {
        sub(/ via RPC/, "", $3);        # strip off postfix
        sub(/^.*\\/, "", $3);           # strip off site prefix
        sub(/\./, "", $12);             # remove trailing period from failures
        if( $12 ~ /[1-9]/) {            # failures > 0
                sub(/^.*@/, "", $15);   # get time of success
                sub(/NTTIME.*$/,"always",$15);# remove NTTIME with always
                errs=errs"\n"$3" has "$12" syncing "$1" since"$15;  #reformat
                sub(/ consecutive.*$/, "", $12);# reduce $12 to error count
                total = total + $12; # total error count
    } else if ( $9 !~ /NTTIME/ ){   # Successes (ignoring unattempted)
                sub(/^.*@/, "", $9);    # get time of success
                sub(/was.*$/,"",$9);    # remove "was successful"
                out=out$3" - "$1" - "$9"\n";    # add to output
     }
        lines = lines + 1;              # count output lines
} END {
        if ( lines < 5 ) {
                print "CRITICAL: Samba4 not running!";
                exit 2;
        } else if ( total > 10 ) {
                print "WARNING:"errs out;
                exit 1;
        } else {
                print "OK:\n"errs out;
                exit 0;
        }
}'
```

Example Healthy check_drs_repl output

```
OK:
DSA object GUID: ddcda871-524e-48c2-87eb-892234f9f159 - SITE1\DOMAIN-CONTROLLER -
- ==== INBOUND NEIGHBORS ==== -
SITE2-DC2 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:31 2018 EDT
SITE4-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:31 2018 EDT
SITE3-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:31 2018 EDT
SITE5-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:31 2018 EDT
SITE6-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:32 2018 EDT
SITE2-DC2 - DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:29 2018 EDT
SITE4-DC1 - DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:29 2018 EDT
SITE3-DC1 - DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:29 2018 EDT
SITE5-DC1 - DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:30 2018 EDT
SITE6-DC1 - DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM - Wed Jun 6 10:41:30 2018 EDT
```

Example Warning check_drs_repl output

WARNING:
SITE-DC3 has 13 consecutive failure(s) syncing CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM since Sun Jun 3 11:07:40 2018 CDT
SITE-DC3 has 13 consecutive failure(s) syncing DC=ForestDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM since Sun Jun 3 11:07:36 2018 CDT
SITE-DC3 has 13 consecutive failure(s) syncing DC=SAMDOM,DC=EXAMPLE,DC=COM since Sun Jun 3 11:07:41 2018 CDT
SITE-DC3 has 13 consecutive failure(s) syncing DC=DomainDnsZones,DC=SAMDOM,DC=EXAMPLE,DC=COM since Sun Jun 3 11:07:38 2018 CDT
SITE-DC3 has 13 consecutive failure(s) syncing CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM since Sun Jun 3 11:07:43 2018 CDT
DSA object GUID: 103d5a2d-5c53-44a8-8f72-a07ad07d9e6b - SITEORP\SITE-DC4 -
 - ==== INBOUND NEIGHBORS ==== -
SITE11-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Sun Jun 3 12:15:09 2018 CDT
SITE-DC1 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Sun Jun 3 12:16:51 2018 CDT
SITE-DC2 - CN=Schema,CN=Configuration,DC=SAMDOM,DC=EXAMPLE,DC=COM - Sun Jun 3 12:15:24 2018 CDT

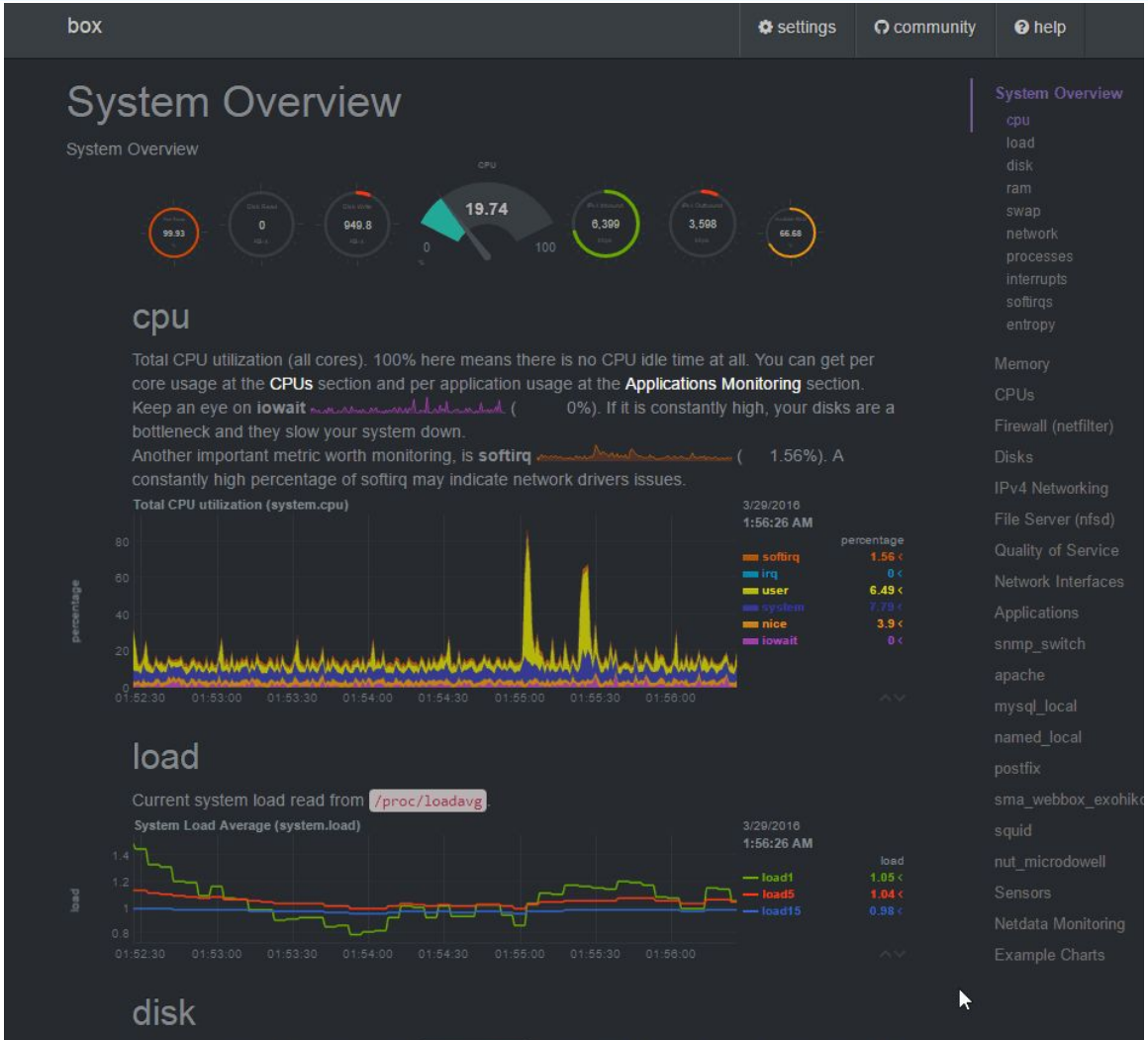
Nagios

- LDAP
  - /usr/lib64/nagios/plugins/check_ldap -H localhost -b "dc=samdom,dc=example,dc=com" -D"dj@samdom.example.com" -P REDACTED
- DNS
  - /usr/lib64/nagios/plugins/check_procs -C named -c1:
  - /usr/lib64/nagios/plugins/check_dns -H host.example.com -w1 -c3

Netdata

- https://github.com/firehol/netdata
- “netdata collects several thousands of metrics per device. All these metrics are collected and visualized in real-time.”

Netdata


box
settings
community
help
System Overview
System Overview
CPU
99.93
0
949.8
19.74
0
100
6,399
3,598
66.68
cpu
Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the CPUs section and per application usage at the Applications Monitoring section.
Keep an eye on iowait (0%). If it is constantly high, your disks are a bottleneck and they slow your system down.
Another important metric worth monitoring, is softirq (1.56%). A constantly high percentage of softirq may indicate network drivers issues.
Total CPU utilization (system.cpu)
3/29/2016
1:56:26 AM
percentage
softirq 1.56
irq 0
user 6.49
system 7.79
nice 3.9
iowait 0
load
Current system load read from /proc/loadavg.
System Load Average (system.load)
3/29/2016
1:56:26 AM
load
load1 1.05
load5 1.04
load15 0.98
disk
System Overview
cpu
load
disk
ram
swap
network
processes
interrupts
softirqs
entropy
Memory
CPUs
Firewall (netfilter)
Disks
IPv4 Networking
File Server (nfsd)
Quality of Service
Network Interfaces
Applications
snmp_switch
apache
mysql_local
named_local
postfix
sma_webbox_exohiko
squid
nut_microdowell
Sensors
Netdata Monitoring
Example Charts

netdata is a **monitoring agent**: you install it on all your systems:
- supports **auto-detection** and **zero configuration** for most applications and systems
- is **real-time**: every metric is on your dashboard in just 1-second (collection to visualization)
- is **fast**: for a few thousand metrics per second, it needs just 1% CPU of a single core
- and **efficient**: it needs a few MB of RAM and no disk I/O at all while it runs
- also, it is **embeddable**, **extensible**, and **open-source** (GPL v3+)

...and netdata runs everywhere:

netdata
simple. effective. awesome!
https://my-netdata.io

Prometheus

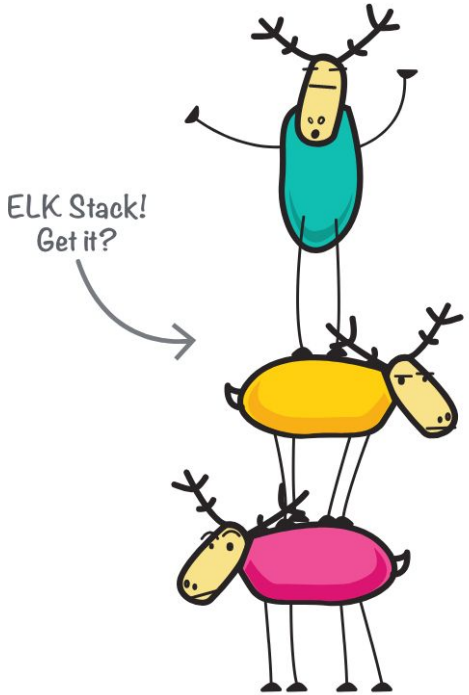
- https://prometheus.io/
- Time series database
- Central repository for netdata data

Grafana

- https://grafana.com/
- “No matter where your data is, or what kind of database it lives in, you can bring it together with Grafana. Beautifully.”
- Can pull from Zabbix, Prometheus, ElasticSearch
- Calculates Domain Jackedness Factor

Elastic.co

- http://elastic.co
- “ELK” stack
  - Filebeat
  - Logstash
  - Elasticsearch
  - Kibana



E Elasticsearch

L Logstash

K Kibana

Filebeat

- https://www.elastic.co/products/beats
- Filebeat is a lightweight log data shipper
- Prospectors monitor log files, converts to json and ships to desired output.

```
- input_type: log
  paths:
    - /var/log/log.samba.json
  fields_under_root: true
  fields:
    tags: ['json']
```

```
multiline:
   pattern: '^20'
   negate: true
   match: after
   max_lines: 4000
 tail_files: false
```

Logstash

- https://www.elastic.co/products/logstash
- “Logstash is an open source, server-side data processing pipeline that ingests data from a multitude of sources simultaneously, transforms it, and then sends it to your favorite “stash.” (Ours is Elasticsearch, naturally.)”
- Log transformation and data extraction

Logstash grok filters:

- Turning this:

```
[2018/03/07 11:50:07.827974,  2]
../auth/auth_log.c:760(log_authentication_event_human_readable)

  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[i-109750$@SAMDOM.EXAMPLE.COM] at [Wed, 07 Mar 2018 11:50:07.827966
IST] with [(null)] status [NT_STATUS_NO_SUCH_USER] workstation [(null)]
remote host [ipv4:10.218.43.15:59902] mapped to [(null)]\[(null)]. local
host [NULL]
```

Logstash

- into this:

```
{datetime: 2018/03/07 11:50:07.827974

samba_source_line:  ../auth/auth_log.c:760

samba_source_function: log_authentication_event_human_readable

authentication_type: Kerberos

…

}
```

Elasticsearch

- https://www.elastic.co/products/elasticsearch
- “Elasticsearch is a distributed, RESTful search and analytics engine capable of solving a growing number of use cases. As the heart of the Elastic Stack, it centrally stores your data so you can discover the expected and uncover the unexpected.”
- Very simple to manage and scale

Kibana

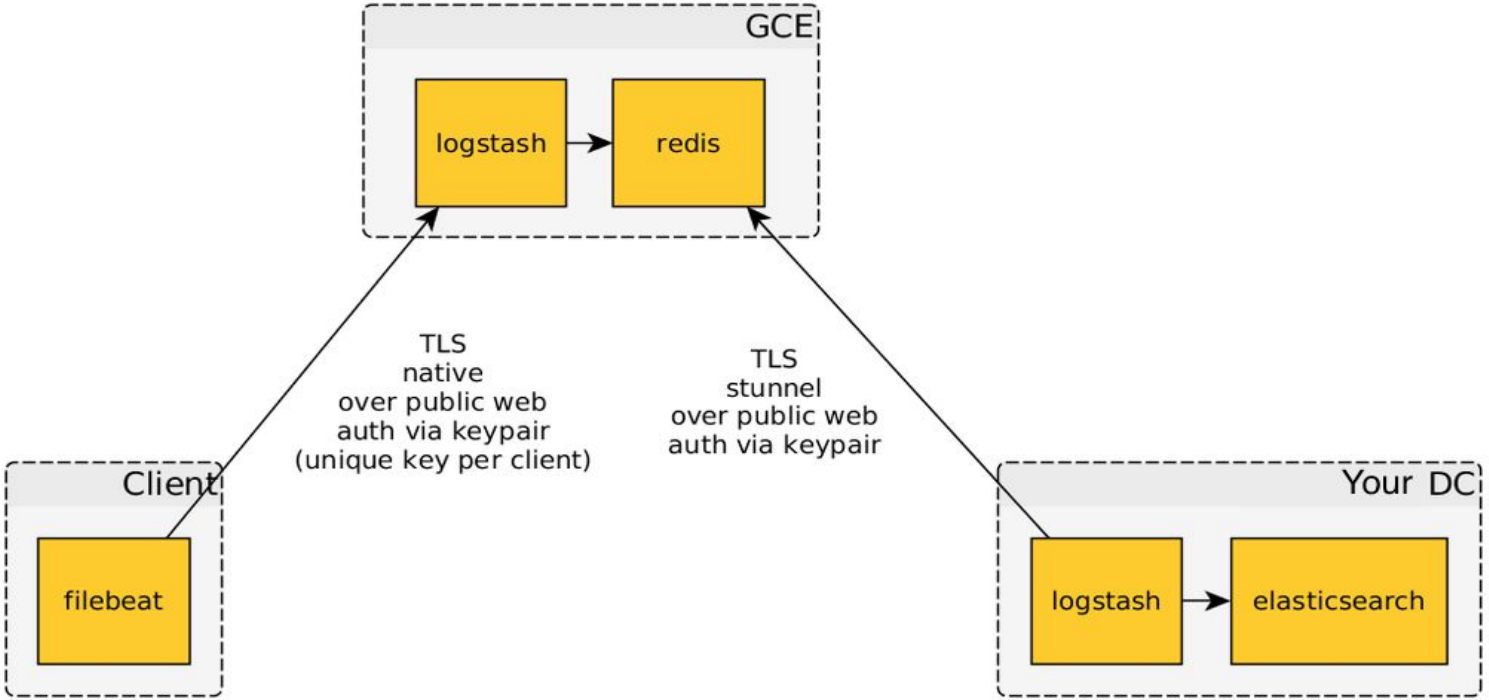
- https://www.elastic.co/products/kibana
- “Kibana lets you visualize your Elasticsearch data and navigate the Elastic Stack, so you can do anything from learning why you're getting paged at 2:00 a.m. to understanding the impact rain might have on your quarterly numbers.”
- Powerful, flexible visualization tool for ElasticSearch (only)

ElastAlert

- https://elastalert.readthedocs.io/en/latest/
- “Easy & Flexible Alerting With ElasticSearch”
  - “Match where there are X events in Y time” (`frequency` type)
  - “Match when the rate of events increases or decreases” (`spike` type)
  - “Match when there are less than X events in Y time” (`flatline` type)
  - “Match when a certain field matches a blacklist/whitelist” (`blacklist` and `whitelist` type)
  - “Match on any event matching a given filter” (`any` type)
  - “Match when a field has two different values within some time” (`change` type)

Multiple domains over multiple networks?

- Use the cloud!



Configuration Management

Puppet

- https://puppet.com
- Configuration management
- Includes an internal CA and basic cert handling
- Puppet Forge: https://forge.puppet.com/kakwa/samba

The Foreman

- https://www.theforeman.org/
- External node classifier
- Ability to set parameters on a variety of conditions
- GUI interface for fact collection

Managing Replication with KCC

The Power of Three (or n+1 where n=2)

- Group sites geographically into triplets
- Create intersite links to connect these small groups

The not-too-distant future of Samba

Better testing

- “Lab” Domain
  - backup/rename of existing domain to preserve scale and number of objects to better mirror our production domain

Better testing

- “Lab” Domain
  - backup/rename of existing domain to preserve scale and number of objects to better mirror our production domain
- Production workload emulation with `traffic_replay`

Better KCC

- Why can’t the domain update link costs automatically based on site to site latency?

Better KCC

- Why can’t the domain update link costs automatically based on site to site latency?
- Why do I need to limit the number of replication partners?
  - Can’t it limit the active links to only what’s needed?

Better KCC

- Why can’t the domain update link costs automatically based on site to site latency?
- Why do I need to limit the number of replication partners?
  - Can’t it limit the active links to only what’s needed?
- If a bridgehead server isn’t specified in a site, it becomes an island.

Thank you

Thank you

- Microsoft
- Catalyst
- SerNet
- Samba Team and community


Q & A