



# eDirectory: Performance tuning and troubleshooting

Rodrigo Gómez  
October 2021

# Agenda

- Search Performance
- Update/write performance
- Avoiding resource starvation
- Q&A



# Search Performance

# Search Performance

- Searches in eDirectory can be done via LDAP or directly via NCP. Example of the later ones are searches with iManager or by IDM drivers.
- The two main factors that influence the search performance are:
  - eDirectory cache configuration
  - Index configuration
- Let's time some searches...

# Search Performance – Sufficient cache

**Database Information**

DIB Size (KB)	813,172
DB Block Size (KB)	4

[View Current Transaction ID](#)

**Database Cache**

	Total	Entry Cache	Block Cache
Maximum Size (KB)	1,500,031	750,016	750,015
Current Size (KB)	999,424	723,584	275,840
Items Cached	233,770	167,380	66,390
Old Versions Cached	0	0	0
Old Versions Size (KB)	0	0	0

**Database Cache Statistics**

Hits	537,214	30,800	506,414
Hit Looks	592,785	37,648	555,137
Faults	233,774	167,384	66,390
Fault Looks	290,052	223,472	66,580
Requests Serviced from Cache (%)	69	15	88

[Clear Statistics](#)

**Database Cache Configuration**

Note: Allocate database cache after considering the file system cache and the available RAM (see documentation for detailed guidelines)

Dynamic Adjust

Cache Adjust Percentage  % of Available Memory

Cache Size Constraints >  KB < Total Available Memory -  KB

---

Hard Limit

Cache Maximum Size  KB

---

Block Cache Percentage  %

Cache Adjust Interval  secs

Cache Cleanup Interval  secs

Cache Settings Permanent

- Lab setup: 100K users, 80K roles
- DIB size is 490Mb, sufficiently large cache.
- Search to be performed is:

```
time ldapsearch -x -D "cn=admin,ou=sa,o=system" -w novell -LLL -b "" -s sub "directReports=*" 1.1
```

- Result with cold cache:
  - real 0m7.436s
- Result with warm cache:
  - real 0m0.245s
- The screenshot shows the cache view right after the first search is performed

# Search Performance – Cache too small

**Database Information**

DIB Size (KB)	813,172
DB Block Size (KB)	4

[View Current Transaction ID](#)

**Database Cache**

	Total	Entry Cache	Block Cache
Maximum Size (KB)	200,000	100,000	100,000
Current Size (KB)	199,936	99,968	99,968
Items Cached	38,792	14,913	23,879
Old Versions Cached	8	4	4
Old Versions Size (KB)	30	14	16

**Database Cache Statistics**

Hits	11,186,188	34,675	11,151,513
Hit Looks	24,306,038	48,467	24,257,571
Faults	5,413,862	3,769,395	1,644,467
Fault Looks	8,152,495	3,779,384	4,373,111
Requests Serviced from Cache (%)	67	0	87

**0 cache hit ratio!**

**Database Cache Configuration**

Note: Allocate database cache after considering the file system cache and the available RAM (see documentation for detailed guidelines)

Dynamic Adjust

Cache Adjust Percentage  % of Available Memory

Cache Size Constraints >  KB < Total Available Memory -  KB

Hard Limit

Cache Maximum Size  KB

- Cache reduced to 200Mb
- Result with cold cache:
  - real 0m2.318s
- Result with warm cache:
  - real 0m2.297s
- Requests serviced from cache drops to 0 and stays below 10
- Performance is close to 15 times worst. The cache can never be fully initialized.

# eDirectory cache configuration

- Two subsystems:
  - Entry cache: Caches entries as they are represented in eDirectory – Prefer for reads
  - Block cache: Caches entries as they are stored in disk – Prefer for writes
- It can be modified via iMonitor -> Agent Configuration -> Database Cache. Changes take effect immediately
- Cache configuration is stored in the `_ndsdb.ini` file
- Rule of thumb: start with 2 times dib size, up to 4 Gb. Increase/decrease based on performance.
- Block cache percentage can be used to distribute the allocated space.

# Search Performance – Index added

- Add relevant index:

```
ndsindex add -D cn=admin,ou=sa,o=system -w
novell -s cn=vm-demohb,ou=servers,o=system
'DirectReportsIx;directReports;value'
```

- Check it's online:

The screenshot shows the Novell Directory Manager interface. At the top, the server and identity information is displayed: **Server:** .CN=vm-demoHB, OU=servers, O=system, T=VM\_DEMOHB\_TREE. **Identity:** .CN=admin, OU=sa, O=system, VM\_DEMOHB\_TREE.

The main area shows the configuration for the **indexDefinition**. The index name is **DirectReportsIx**, and it is currently **Present** with a **Version** of **0** and is **Aliased**. The **TimeStamp** is **11/12/18 02:32:47 PM 1:33**.

Below the index definition, a table shows the status of various indices:

Present	0	DirXML-Policies	online	value	system	server add	DirXML-Policies
Not Present	0	DirectReportsIx	bringing online (low)	value	user defined	server add	directReports
Present	0	DirectReportsIx	online	value	user defined	server add	directReports

- Cache size is now less relevant

- Search result:

- real 0m0.017s

- Tracing that the index is being used with the +RECM (ndstrace) or Storage Manager tag

```
base: ""
scope:2 dereference:0 sizelimit:0 timelimit:0 attrsonly:0
filter: "(directReports=*)"
attribute: "1.1"
16:43:41 80290700 STEMAN: Iter #2162b350 query ((Flags&1)==1) && (((((directReports$626A$.Flags&8)==8) && directReports$626A$.Flags&8)) && ( <+
16:43:41 80290700 STEMAN: Iter #2162b350 query ++> AncestorID=32797))
16:43:41 80290700 STEMAN: Iter #2162b350 index = DirectReportsIx$IX$2672
16:43:41 80290700 STEMAN: Iter #2162b350 first( eid=143068)
16:43:41 80290700 LDAP: (127.0.0.1:34688)(0x0002:0x63) Sending search result entry "cn=gerard,ou=users,o=data" to connection 0x12101180
```



# Adding an index – monitor progress

- The limber process starts the index addition. Progress can then be followed with the +RECM trace
- The index gets first added to the NCP Server object.
- Then it gets copied over to the [Pseudo Server] object, which can be accessed via iMonitor -> Agent Configuration
- From there, the operations is passed down to Flaim.
- The index goes through different stages until it becomes Online

# Indexes

- An index is a set of keys arranged in a way that significantly speeds up the task of finding any particular key within the index.
- Constructed based on values of attributes in the entries
- Maintained in memory in the block cache
- eDirectory defines a default set of indexes for system attributes like parentID or ancestorsID
- Default indexes are defined for attributes such as CN, Surname and Given Name

# Indexes – cont.

- Indexes can be of type presence, value, and substring.
  - Presence indexes are only used for presence filters (i.e. cn=\*)
  - Substring indexes create a value indexes with all substring combinations of each value, which makes them very expensive
- System creates automatically an index if there are more than 25 values of a given attribute or if any value is larger than 2048 bytes
  - This behavior can be disabled with `disablemovetoattrcontainer =1` in the `_ndsdb.ini` file
  - Attributes then are shown in the Pseudo Server object in the **dsContainerReadyAttrs**
  - You can see if the index has been added automatically in iMonitor. Index type is “system”
  - System indexes are stored in a separate location by Flaim

# Compound indexes

- Compound indexes can be created to combine attributes
  - IDM (Identity Apps) creates by default a series of them
  - Compound indexes are always value indexes
  - It is not possible to combine an attribute that has been added as a System index
- The parameter `-a` in `ndsindex` adds `AncestorsID` information to the index information (from eDir 9.1)
  - The index is displayed as a compound index with the attributes defined plus `AncestorsID` as an extra attribute to the attribute list

# Other factors that affect search performance

- LDAP search controls like VLV, Server Side Sort and Paged Search force the use of specific indexes, impacting performance
- Member queries on paths that contain dynamic groups will spawn a new search for each dynamic group
- Alias objects can have a big performance impact. Reduce the use in search intensive trees
- Complex ACL calculations can have an impact on the search performance as well



**Update/write performance**

# Avoid unnecessary writes - Login Update Interval

- On each login, attribute Login Time is updated and the previous value is copied to Last Login Time -> Overkill for LDAP Binds
- It's possible to control this behavior with the attribute `sasUpdateLoginInfo`:
  - **0 or off**: Do not update any login attributes.
  - **1**: Only update attributes that are required by intruder detection.
  - **2**: Update all login attributes except unused user password policy attributes.
  - **3 or on**: Update all login attributes.
- The frequency of update is controlled by `sasUpdateLoginTimeInterval`:
  - If the value is between **1** and **1440** minutes, the Login Time attribute is updated after the specified interval. The Last Login Time attribute will not be updated.

# Login Update Interval

- Can be specified at:

- User
- Container of the user
- Partition root
- Login Policy -> Tree wide

- Or at server level:

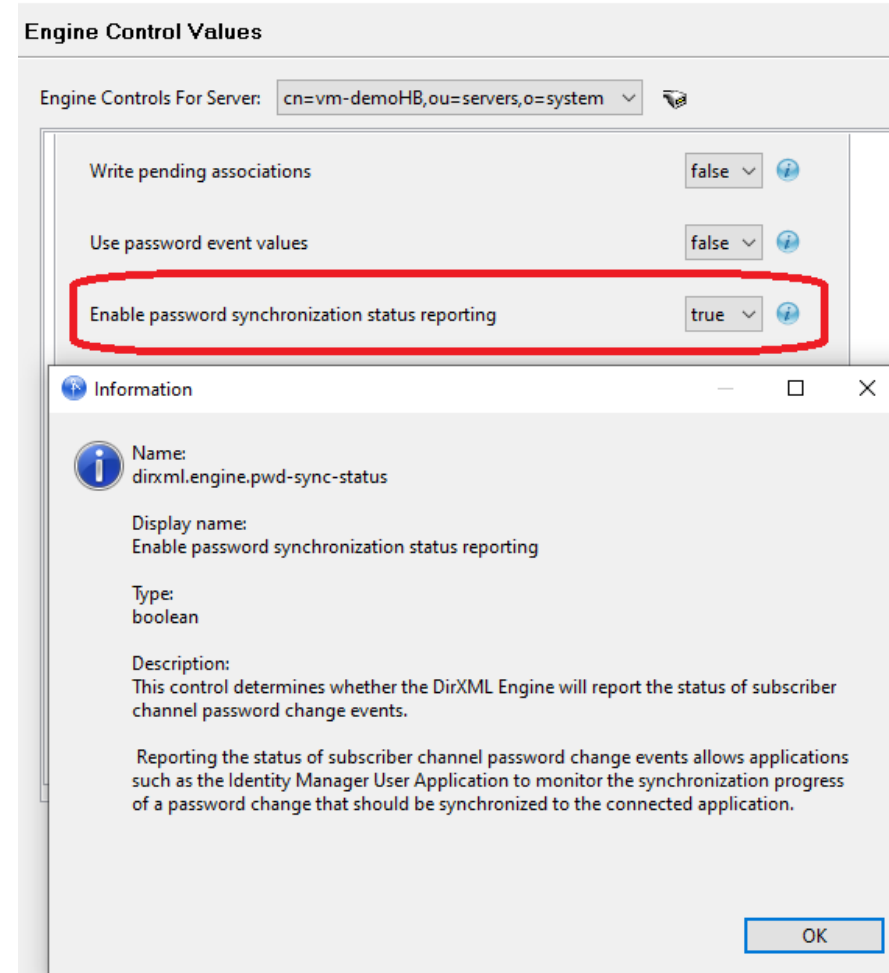
```
#cat /var/opt/novell/eDirectory/data/nmas.config  
nmas LoginInfo 2  
Nmas UpdateLoginTimeInterval 30
```

- **NDSD\_TRY\_NMASLOGIN\_FIRST** needs to be set for LDAP Binds




# Identity Manager – DirXMLPasswordSyncStatus

- This attribute is used for the functionality present in iManager -> Check Password Sync status
  - The function reads this attribute and reports the status for each connected system with this setting enabled.
- If this feature is not being used, the tracking of password sync status can be disabled with an Engine Control Value on a per driver basis.



# Identity Manager - DirXMLStatusLog



- Avoid updating the Dirxml-StatusLog attribute
- The attribute stores in eDirectory the last status results, information that can be retrieved as well from a log at level 0
- The attribute is not synchronized to other servers, but it causes the modifiersName and Revision attributes to be updated.

Modify Object:  driverset1.system

Identity Manager | General

Named Passwords | Global Config Values | **Log Level** | Status Log | Activation | Misc | Inspector

### Log Level

- Log errors
- Log errors and warnings
- Log specific events 
- Log XDAS events 
- Only update the last log time
- Logging off
- Turn off logging to Driver Set, Subscriber and Publisher logs.

Maximum number of entries in the log (50 - 500):

# Update Performance – Write locks

The screenshot shows the NDS iMonitor Agent Activity window. The title bar indicates the date and time: Sat Feb 29 17:18:24 2020. The main window displays the following information:

**Refresh Settings:**  
Refresh Off  
Refresh Interval: 15 seconds  
Update

**Activity:**  
Verbs: Activity, Statistics  
Synchronization: Current, Schedule  
Events: Activity, Statistics, Rights  
Background Process Schedule

**Links:**

**DIB Writer Info**

Total Writers	Verb/Process	Time (ms)	Thread ID
5	DSAModifyEntry	42872	7FD96700
	DSAModifyEntry	24181	773EC700
	Unregistered	18495	6FD86700
	DSAConsole	12191	76C98700
	DSAModifyEntry	5190	AF490700


**Verb/Process Statistics**

	Verb/Process	Active
9	0x9 Modify Entry	3
93	0x5d Statistics	1
99	0x63 Console	1
-2	0xffffffe BK_SKULKER	1
-86	0xfffffaa Local Login	1
-128	0xfffff80 DSV_BK_CPUMONITOR	1
-135	0xfffff79 BK CHANGE CACHE SKULK TRIGGER	1

- iMonitor -> Agent Activity shows information on long write locks
- The image shows a 42 second lock by process DSA Modify Entry
- The Wait column indicates how long other threads have waited for the write lock
- In this situation, it's possible that too many threads get spawned and the server runs out of threads.
- Identify what is causing the write lock. Usual suspects: DirXML-EntitlementResult, DirXML-StatusLog, pwdFailureTime

# Update Performance – High Value count report

## Report

Value Count 

### Value Count More than 500

Object Name or Attribute Name	Value Count
CN=ABBY_ADOMAITIS,OU=users,O=data,T=VM_DEMOHOB_TREE, Group Membership	10001
Security Equals	10004
CN=LORNA_TRINH,OU=users,O=data,T=VM_DEMOHOB_TREE, DirXML-EntitlementResult	4890
CN=SOD role 2,CN=Level30,CN=RoleDefs,CN=RoleConfig,CN=AppConfig,CN=User Application Driver,CN=driverset1,O=system,T=VM_DEMOHOB_TREE, Equivalent To Me	109579
CN=bartgrp,OU=groups,O=data,T=VM_DEMOHOB_TREE, Member	20011
Equivalent To Me	20011
CN=bandries,OU=users,O=data,T=VM_DEMOHOB_TREE, Group Membership	10004
Security Equals	10005

- iMonitor -> Reports -> Value count
- Updating attributes with large value counts is very resource intensive. Updating indexes takes a long time, specially for large values
- Latest versions of RRSD driver limit how long DirXML-EntitlementResult values are stored
- It is best to avoid a high value count condition. Plan resource/group assignment accordingly.

# Tuning eDirectory Background processes

Background Process Interval (minutes)			
<input type="text" value="780"/>	Backlink/DRL Interval	<input type="text" value="720"/>	Cleaner Interval
<input type="text" value="60"/>	Outbound Sync Interval	<input type="text" value="240"/>	Schema Sync Interval
<input type="text" value="2"/>	Janitor Interval	<input type="text" value="30"/>	Purger Interval

**Configure Advanced Referral Costing**

Disable  
 Enable  
 Debug

**Asynchronous Outbound Synchronization Settings**

Enable  Disable

Async Dispatcher Thread Delay (ms)

**Background Process Delay Settings**

CPU

Maximum CPU Utilization %  Maximum Delay Limit (ms)

---

Hard Limit

Change Cache Processing Delay (ms)  Purger Delay (ms)

ObitProc Delay (ms)

- iMonitor -> Agent Configuration -> Background Process Settings
- Enable Async Outbound sync to split the process that builds the Change Cache from the one that does the actual sync.
- Make sure ARC is enabled
- Set Delay settings to a value between 10 and 20 ms. A value below 5 ms is not recommended.

# Adjusting synchronization strategies

**Agent Synchronization**

Direction	State	Activation Date	Change State
Inbound	Enabled		<input checked="" type="radio"/> No Change <input type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="24"/> Hours
Outbound	Enabled		<input checked="" type="radio"/> No Change <input type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="24"/> Hours
Inline Change Cache			<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<small>Note: Before disabling Inline Change Cache, disable Outbound and Priority Sync Outbound.</small>			
Synchronization Method			<input type="radio"/> by Partition <input type="radio"/> by Server <input checked="" type="radio"/> Dynamic Adjust
System Computed Synchronization Threads			<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Max. System Computed Synchronization Threads			<input type="text" value="8"/>
Max. Manual Setting Synchronization Threads			<input type="text" value="8"/>
Priority Sync Outbound			<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Priority Sync Inbound			<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Priority Sync Threads			<input type="text" value="4"/>
Priority Sync Queue Size			<input type="text" value="-1"/>
<input type="button" value="Submit"/>			

- iMonitor -> Agent Configuration -> Agent Synchronization
- Consider reducing the number of threads, to reduce contention
- If one server updates more, set that server with a higher amount of threads
- Priority sync can help for time sensitive data, like passwords, but it shouldn't be abused.



# Avoiding resource starvation

# Thread pool

- Instead of creating and destroying threads, they are placed in a pool.
- Two types of queues:
  - Ready queue
  - Waiting queue
- Use `ndstrace -c threads` to gather:
  - The total number of threads that are spawned, terminated, and idle.
  - The total number of worker threads currently and the peak number of worker threads.
  - The number of tasks and peak number of tasks in the Ready queue.
  - The minimum, maximum and average number of microseconds spent in the Ready queue.
  - The current and maximum number of tasks in the Waiting queue.



# Thread pool parameters:

- **n4u.server.max-threads:** Maximum number of threads that can be available in the pool.
- **n4u.server.idle-threads:** Maximum number of idle threads that can be available in the pool.
- **n4u.server.start-threads:** Number of threads started.
- Use `ndsconfig get/set` or modify `nds.conf` file directly

# Thread pool

- Default max threads is 256
- Maximum with ndsconfig set is 512
- If modified on nds.conf, there is no actual maximum
- Consider that each thread spawned consumes a memory footprint

# Ephemeral ports

- Default Linux range is from 32768 to 61000
  - *To change it: `echo 15000 65000 > /proc/sys/net/ipv4/ip_local_port_range`*
- You can use `netstat -na` to check how many ports are in use. Check for large amount of ports in TIME\_WAIT status
- Parameter `NDSD_AGENT_CONTEXT_OPTIMIZATION=true` should help reduce the need for this
- What works even better is to allow the system to reuse threads in Time Wait status:
  - Dynamic: `echo 1 > /proc/sys/net/ipv4/tcp_tw_reuse`
  - Permanent: *add `net.ipv4.tcp_tw_reuse = 1` in file `sysctl.conf`*

# eDirectory contexts

- iMonitor -> Connections -> Contexts
- Different processes inside eDirectory spawn eDirectory contexts
- The table is limited by the NCP buffer size, which limits it to 32K
- If the table is full, the server stops working
- This is often a symptom of a software bug.

Connections:		Context											
		Context	Identity	ID Handle	Connection	Remote		Create Time		Build Number	Module		
					Type	Address	Conn ID	Task ID			Module Handle	Module Name	Name
<b>Inbound</b>	<a href="#">Connections</a>	0	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	3		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Iterations</a>	1	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
<b>Outbound</b>	<a href="#">Connections</a>	2	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Identities</a>	3	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Contexts</a>	4	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Bad Addresses</a>	5	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Statistics</a>	6	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Most Recent</a>	7	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
<b>Links:</b>	<a href="#">Agent Summary</a>	8	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Agent Synchronization</a>	9	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Known Servers</a>	10	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Schema</a>	11	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Agent Configuration</a>	12	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Trace Configuration</a>	13	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Agent Health</a>	14	.vm-demoHB.servers.system.VM_DEMOHB_TREE.	0	1		0	0	02/29/20 03:05:34 PM		0000010C	/opt/novell/eDirectory/lib64/nds-modules/libdxevent.so.3	
	<a href="#">Agent Process Status</a>												

# Transaction ID

- Before it's exhausted in ndsd.log and with the flag +RECM:  
**FATAL: DB : WARNING: the last transaction ID 0XXXXXXXXX**
- Once exhausted, the error displayed is:  
**The current transaction ID is 0XXXXXXXXX. Run local database repair with rebuild database option enabled**  
**Transaction ID has exceeded the allowed limit of 0xFFFFE000. Run local database repair**
- More information in TID 7002658  
<https://support.microfocus.com/kb/doc.php?id=7002658>

# TasksMax=infinity

- With the introduction of systemd (SLES 12/RHEL7), startup is controlled by unit file
- In `/etc/systemd/system/multi-user.target.wants` resides a symlink:
  - `ndsdtmpl-etc-opt-novell-eDirectory-conf-nds.conf@-etc-opt-novell-eDirectory-conf-env.service -> /usr/lib/systemd/system/ndsdtmpl-etc-opt-novell-eDirectory-conf-nds.conf@.service`
- In `/usr/lib/systemd/system` resides the actual file, created from the template stored in the `conf` directory
- From SLES 12 SP1, the OS imposes a limit of 512 tasks (threads) per process. This can be avoided adding this entry to Unit file:
  - `TasksMax=infinity`
- One of the symptoms of this problem is that it's not possible to start more than 25 drivers in a server
- Others are random crashes when the server is highly utilized.

# Cleaning the oidpInstanceData attribute

- oidpInstanceData stores session information for Identity Applications.
- If a session is not closed cleanly (close browser without logout), it grows over time. If it grows too large, logins will fail with error -649: Insufficient buffer
- New property in the UserApp driver will perform automatic cleanup:
  - [https://www.netiq.com/documentation/identity-manager-48/releasenotes\\_idm484/data/new-features-and-enhancements.html#t4dk24tdr44u](https://www.netiq.com/documentation/identity-manager-48/releasenotes_idm484/data/new-features-and-enhancements.html#t4dk24tdr44u)

# More information

- Extended version of this presentation:
  - <https://www.thettp.org/edir-webinar>
- Tuning guide:
  - [https://www.netiq.com/documentation/edirectory-92/edir\\_tuning/data/bookinfo.html](https://www.netiq.com/documentation/edirectory-92/edir_tuning/data/bookinfo.html)
- History of issues fixed:
  - eDir 9: <https://support.microfocus.com/kb/doc.php?id=7016794>
  - eDir 8.8.x: <https://support.microfocus.com/kb/doc.php?id=3426981>





Q&A



**Thank you.**