NIS+ Explained

September 26, 2002

Presented by:
Chris Wong
cwong@cerius.com
Cerius Technology Group, Inc.
http://newfdawg.com

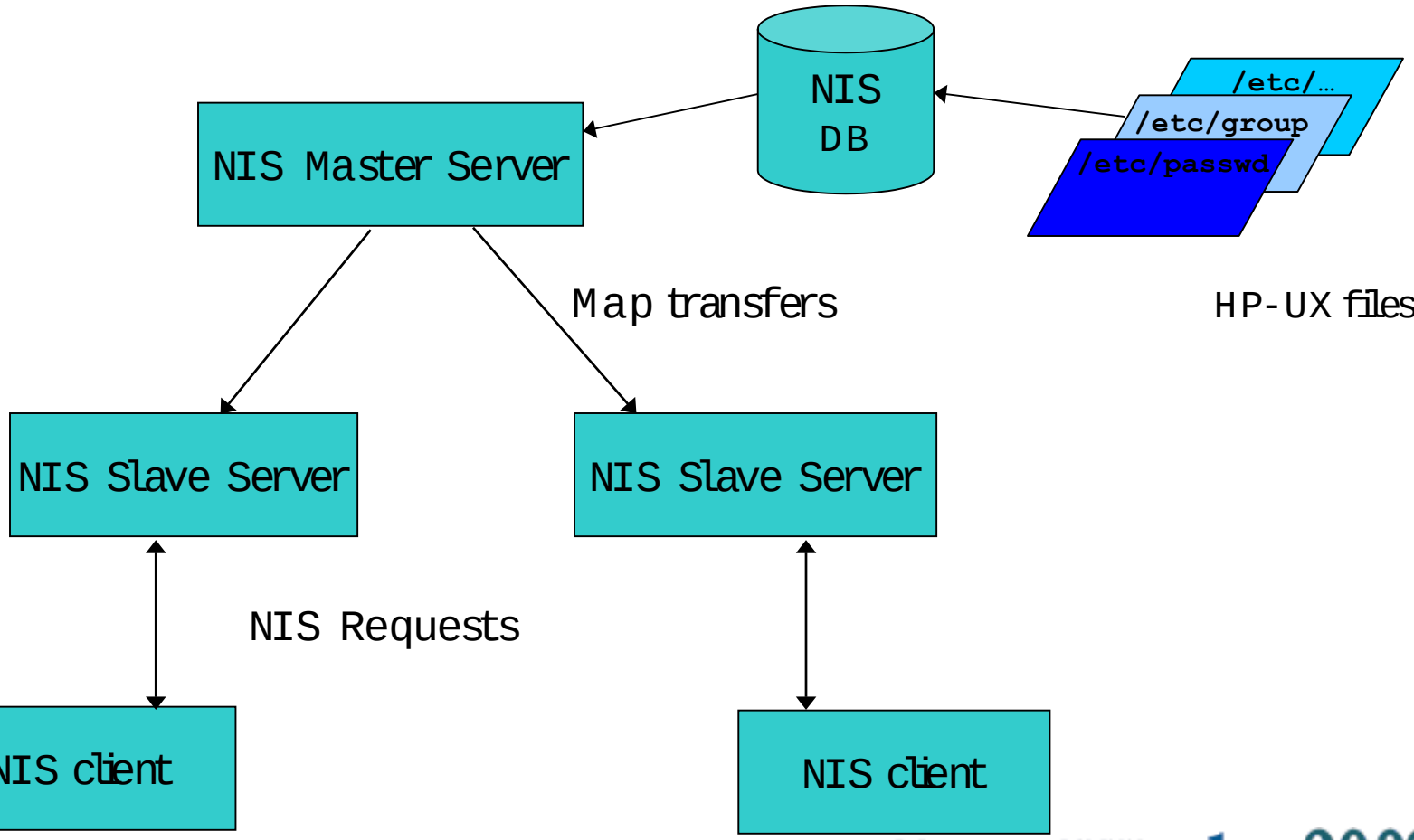
Why?
Shared Information

- Hosts
- IP addresses
- Users
- Passwords
- Protocols and Services
- Timezone

Reasons for Information Systems

- DNS
  - Ability to use common names rather than IP addresses
  - DNS namespace (host to IP resolution and mail delivery) is divided into a hierarchy of domains
- NIS and NIS+
  - Centralize Information
    - Reduce errors
    - Easier administration
  - Collection of ***network*** information is the NIS or NIS+ namespace.

Network Information System (NIS)

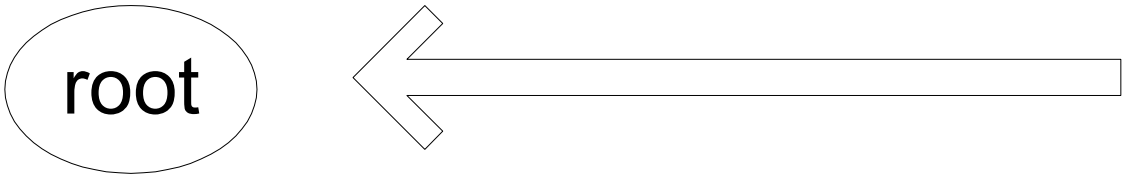


NIS vs. NIS+

- NIS
  - Namespace is flat
  - Uses maps
  - Focused on stability, not replication
  - Focused on static info, not dynamic
- NIS+
  - Namespace is hierarchical
  - Uses tables
  - Designed for large networks (replication)
  - Designed for rapidly changing information
  - Designed to be secure
  - Accepts incremental updates

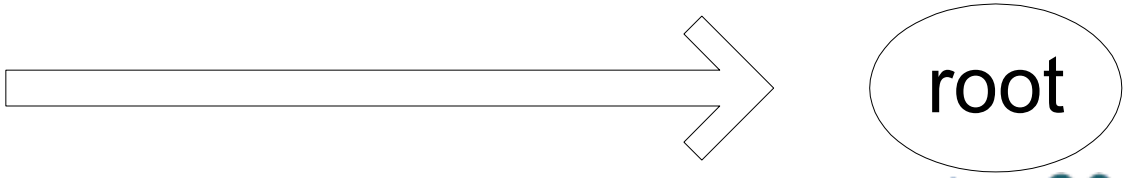
UNIX:

/home/jrice/myfile



NIS+:

florida.cerius.com.



UNIX:

/home/jrice/myfile

Accessed with editors (vi), text manipulators (awk), and many commands (more, rm)

NIS+:

florida.cerius.com.

Never directly accessed!!
Use NIS+ commands or a GUI

UNIX:

/home/jrice/myfile

Directory structure separated by the slash (/")

NIS+:

florida.cerius.com.

Directory structure separated by the dot (.)

UNIX:

/home/jrice/myfile

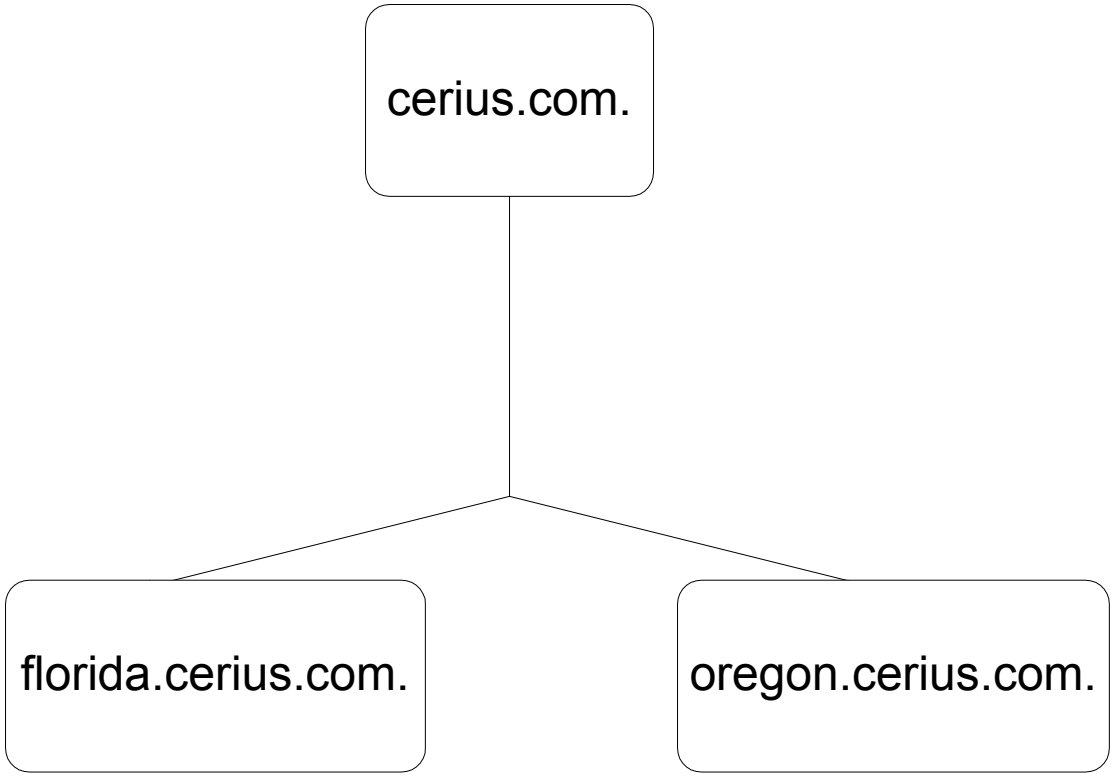
Partial: myfile
Fully qualified: /home/jrice/myfile
or
$HOME/myfile
(Assuming $HOME=/home/jrice)

NIS+:

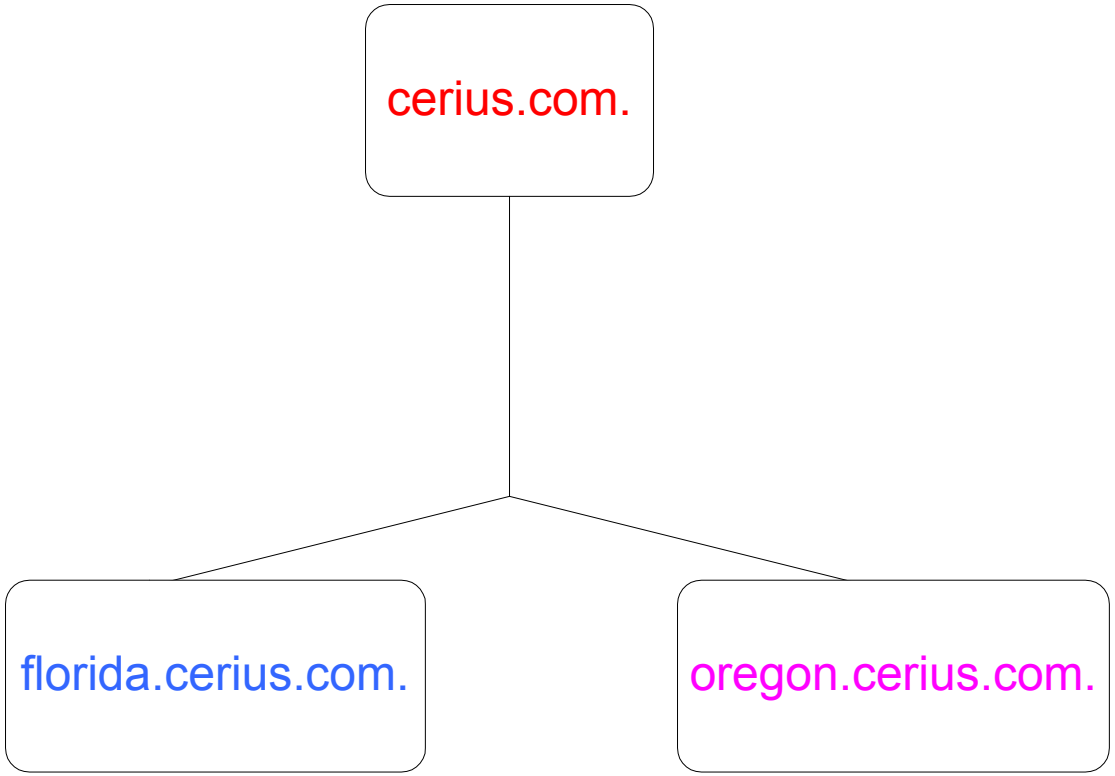
florida.cerius.com.

Partial or simple: florida
Fully qualified: florida.cerius.com.
or
$
(Assuming $=florida.cerius.com.)

The namespace
How many domains?



Three

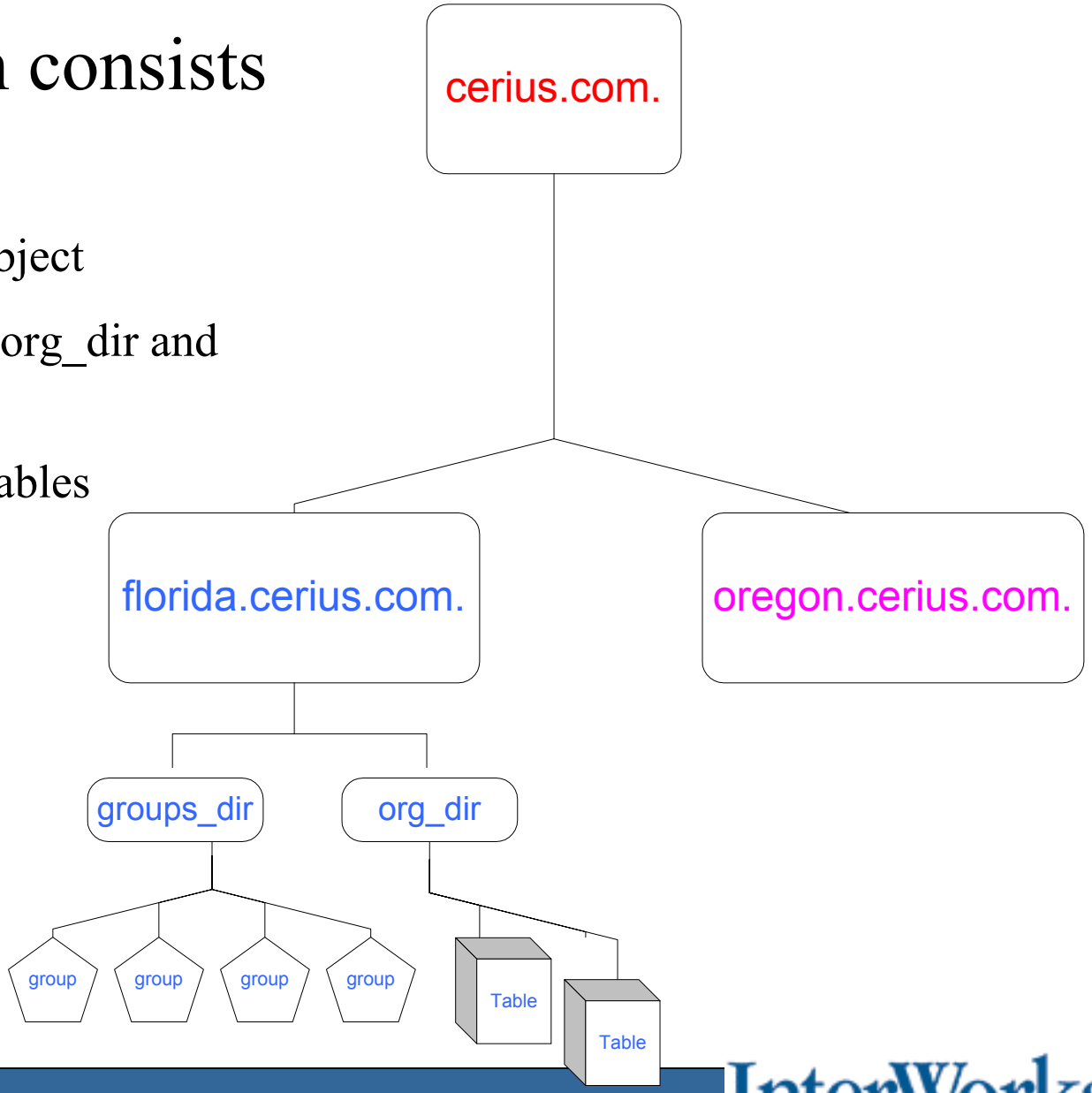


Domain consists of:

Directory Object

Directories: org_dir and group_dir

Groups & Tables



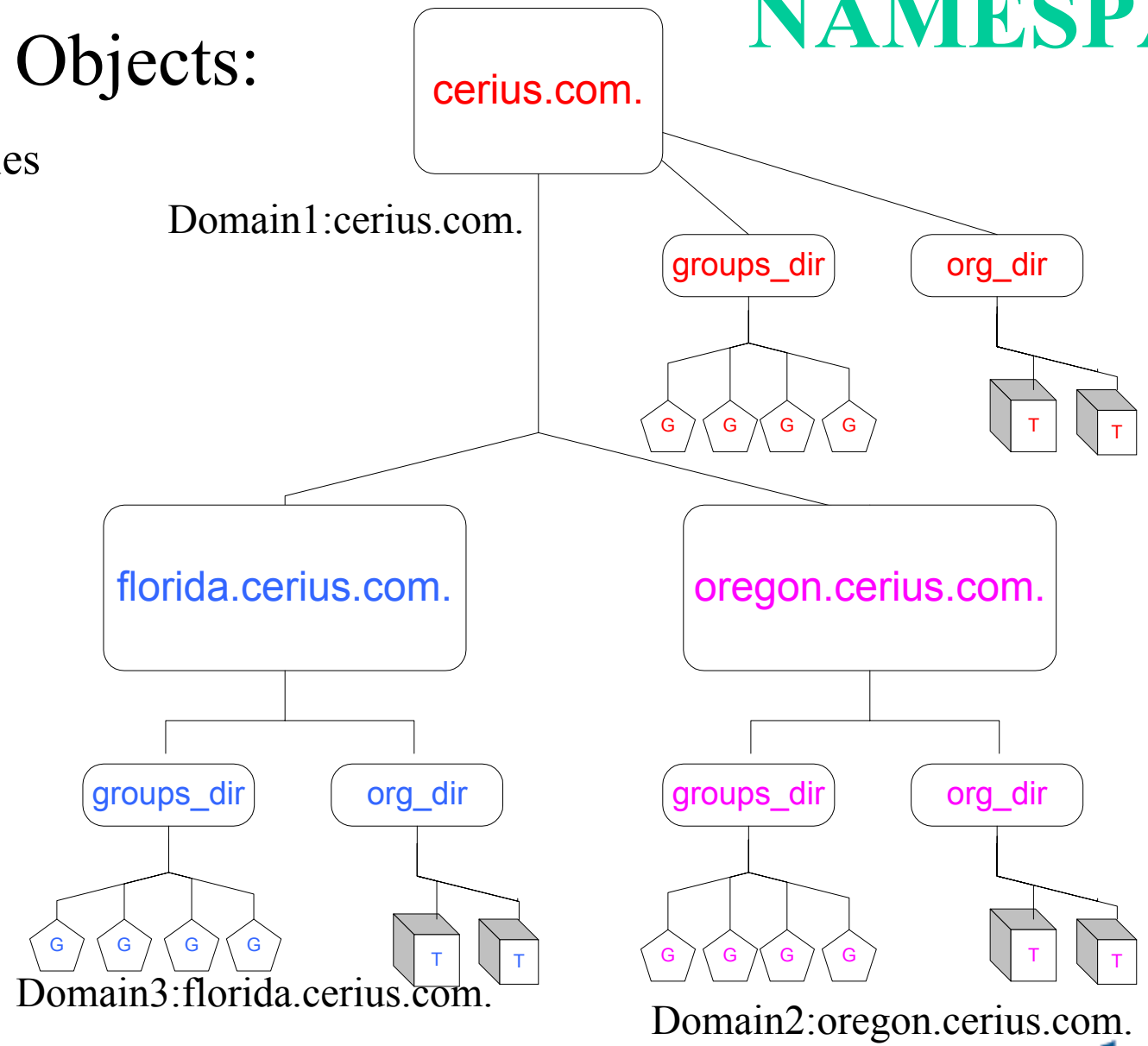
NAMESPACE

NIS+ Objects:

Directories

Tables

Groups



Name Expansion

UNIX:

/home/jrice/myfile

User enters: myfile
Searches through the directories found in the PATH variable

NIS+:

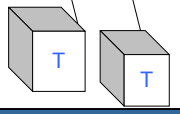
florida.cerius.com.

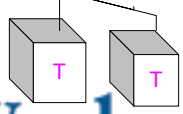
Request for: florida
Searches through the entries found in the NIS_PATH variable
$=default directory
If no NIS_PATH variable is set:
1). Search default domain (client's home domain)
2). Search parent directories in ascending order

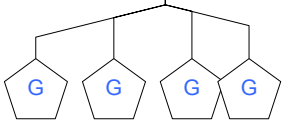
Root domain

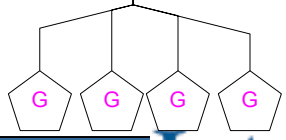
Must contain 2 labels and end with a dot.

Is only a parent.









Step #1: Creating the root master server

- NIS+ commands used:
  - domainname
  - nisserver
  - nisls
  - niscat
  - nisgrpadm
  - nispopulate
  - nisping

Step #1a: Update the PATH variable:

- **ctg500g#: vi /etc/PATH**
- /usr/bin:/usr/ccs/bin:/usr/contrib/bin:/opt/nettladm/bin:/opt/fc/bin:/opt/fcms/bin:/opt/upgrade/bin:/opt/pd/bin:/usr/bin/X11:/usr/contrib/bin/X11:/opt/hparray/bin:/opt/resmon/bin:/opt/perf/bin:/opt/ignite/bin:/opt/OV/bin/OpC:/opt/scr/bin:/opt/mx/bin://opt/perl/bin:/usr/sbin/diag/contrib:/opt/pred/bin**:/usr/lib/nis**
- Relogin or: export PATH=$PATH:/usr/lib/nis

Step #1b: Change startup scripts

- **ctg500g#: vi /etc/rc.config.d/namesvrs**
- NIS_MASTER_SERVER=0
- NIS_SLAVE_SERVER=0
- NIS_CLIENT=0
- **NISPLUS_SERVER=1**
- **NISPLUS_CLIENT=1**
- NIS_DOMAIN=""

Step #1c: Create separate Logical Volume for NIS+ namespace

- ctg500g#: lvcreate -L 100 -n nis vg00
- ctg500g#: newfs -F vxfs /dev/vg00/rnis
- ctg500g#: mkdir /var/nis
- ctg500g#: vi /etc/fstab
  - /dev/vg00/nis /var/nis vxfs delaylog 0 2
- ctg500g#: mountall or manual mount

Step #1d: Set the environment

- **ctg500#: /usr/bin/domainname cerius.com**
- **ctg500#: export NIS_GROUP=admin.cerius.com.**

Step #1e: Create the server

- **ctg500g#: nisserver -r** ***-d cerius.com. (Optional since specified with domainname command)***
- This script sets up this machine "ctg500g" as an NIS+
- root master server for domain cerius.com..
- Domain name : cerius.com.
- NIS+ group : admin.cerius.com.
- NIS (YP) compatibility : OFF
- Security level : 2=DES
- Is this information correct? (type 'y' to accept, 'n' to change) **y**
- This script will set up your machine as a root master server for
- domain cerius.com. without NIS compatibility at **security level 2.**
- Use "nisclient -r" to restore your current network service environment.
- Do you want to continue? (type 'y' to continue, 'n' to exit this script) **y**

```
setting up domain information "cerius.com." ...
setting up switch information ...
running nisinit ...
This machine is in the cerius.com. NIS+ domain.
Setting up root server ...
All done.
starting root server at security level 0 to create
credentials...
running nissetup ...
(creating standard directories & tables)
org_dir.cerius.com. created
groups_dir.cerius.com. created
passwd.org_dir.cerius.com. created          cred.org_dir.cerius.com. created
group.org_dir.cerius.com. created           ethers.org_dir.cerius.com. created
auto_master.org_dir.cerius.com. created     hosts.org_dir.cerius.com. created
auto_home.org_dir.cerius.com. created       mail_aliases.org_dir.cerius.com. created
bootparams.org_dir.cerius.com. created      sendmailvars.org_dir.cerius.com. created
```

netmasks.org_dir.cerius.com. created
netgroup.org_dir.cerius.com. created
networks.org_dir.cerius.com. created
protocols.org_dir.cerius.com. created
rpc.org_dir.cerius.com. created
services.org_dir.cerius.com. created
timezone.org_dir.cerius.com. created
adding credential for ctg500g.cerius.com...
Enter login password: (root99)
Wrote secret key into /etc/.rootkey
setting NIS+ group to admin.cerius.com. ...
restarting root server at security level 2 ...
This system is now configured as a root server for domain cerius.com.
You can now populate the standard NIS+ tables by using the nispopulate script or /usr/lib/nis/nisaddent command.

ctg500g#: ll /var/nis

```
total 76
-rw-r--r--   1 root       sys          308 Nov  8 09:38 NIS_COLD_START
-rw-r--r--   1 root       sys         8192 Nov  8 09:38 NIS_SHARED_DIRCACHE
drwxr--r--   2 root       sys         1024 Nov  8 09:37 ctg500g
-rw-r--r--   1 root       sys         3804 Nov  8 09:37 ctg500g.dict.log
-rw-------   1 root       sys        65537 Nov  8 09:38 ctg500g.log
```

ctg500g#: ll /var/nis/ctg500g

```
total 66
-rw-r--r--   1 root     sys          120 Nov  8 09:37 auto_home.org_dir
-rw-r--r--   1 root     sys          120 Nov  8 09:37 auto_master.org_dir
-rw-r--r--   1 root     sys          120 Nov  8 09:37 bootparams.org_dir
-rw-r--r--   1 root     sys          280 Nov  8 09:37 cred.org_dir
-rw-r--r--   1 root     sys          556 Nov  8 09:37 cred.org_dir.log
-rw-r--r--   1 root     sys          180 Nov  8 09:37 ethers.org_dir
-rw-r--r--   1 root     sys          176 Nov  8 09:37 group.org_dir
-rw-r--r--   1 root     sys          124 Nov  8 09:37 groups_dir
-rw-r--r--   1 root     sys          520 Nov  8 09:37 groups_dir.log
-rw-r--r--   1 root     sys          240 Nov  8 09:37 hosts.org_dir
-rw-r--r--   1 root     sys          204 Nov  8 09:37 mail_aliases.org_dir
-rw-r--r--   1 root     sys          360 Nov  8 09:37 netgroup.org_dir
-rw-r--r--   1 root     sys          180 Nov  8 09:37 netmasks.org_dir
-rw-r--r--   1 root     sys          240 Nov  8 09:37 networks.org_dir
-rw-r--r--   1 root     sys          124 Nov  8 09:37 org_dir
-rw-r--r--   1 root     sys         6028 Nov  8 09:37 org_dir.log
-rw-r--r--   1 root     sys          176 Nov  8 09:37 passwd.org_dir
-rw-r--r--   1 root     sys          248 Nov  8 09:37 protocols.org_dir
-rw-r--r--   1 root     sys          396 Nov  8 09:37 root.object
-rw-r--r--   1 root     sys          124 Nov  8 09:37 root_dir
-rw-r--r--   1 root     sys         2152 Nov  8 09:38 root_dir.log
-rw-r--r--   1 root     sys          248 Nov  8 09:37 rpc.org_dir
-rw-r--r--   1 root     sys          120 Nov  8 09:37 sendmailvars.org_dir
-rw-r--r--   1 root     sys          300 Nov  8 09:37 services.org_dir
-rw-r--r--   1 root     sys           55 Nov  8 09:37 serving_list
-rw-r--r--   1 root     sys          124 Nov  8 09:37 timezone.org_dir
```

nisaddcred des

- **ctg500g#: ll /etc/.rootkey**
  - -rw------- 1 root sys 50 Nov 8 09:37 /etc/.rootkey
- **ctg500g#: more /etc/.rootkey**
  - 63c224fc389017ae571802a7d468465edc5c544eafad4be7

Directories & Groups

- **ctg500g#: nisls –lR**
- cerius.com.:
- **D** r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:38 2001 org_dir
- **D** r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:38 2001 groups_dir
- groups_dir.cerius.com.:
- **G** ----rmcdr---r--- ctg500g.cerius.com. Thu Nov 8 09:37:59 2001 admin

Tables

- org_dir.cerius.com.:
- T ----rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:38 2001 passwd
- T ----rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 group
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 auto_master
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 auto_home
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 bootparams
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 cred
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 ethers
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 hosts
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 mail_aliases
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:39 2001 sendmailvars
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 netmasks
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 netgroup
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 networks
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 protocols
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 rpc
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 services
- T r---rmcdrmcdr--- ctg500g.cerius.com. Thu Nov 8 09:37:40 2001 timezone

nsswitch.conf (NIS+ does not use DNS by default)

- **ctg500g#: more /etc/nsswitch.conf**
- # /etc/nsswitch.nisplus:
- #
- # An example file that could be copied over to /etc/nsswitch.conf; it
- # uses NIS+ (NIS Version 3) in conjunction with files.
- #
- passwd: files nisplus
- group: files nisplus
- hosts: nisplus [NOTFOUND=return] files
- services: nisplus [NOTFOUND=return] files
- networks: nisplus [NOTFOUND=return] files
- protocols: nisplus [NOTFOUND=return] files
- rpc: nisplus [NOTFOUND=return] files
- publickey: nisplus
- netgroup: nisplus [NOTFOUND=return] files
- automount: files nisplus
- aliases: files nisplus

2 daemons started

- ctg500g#: ps –ef | grep nis
  - –**/usr/sbin/rpc.nisd**
  - –**/usr/sbin/nis_cachemgr**

The group domain was added automatically

- **ctg500g#: niscat -o admin.groups_dir.cerius.com.**
- Object Name : admin
- Owner : ctg500g.cerius.com.
- Group : **admin.cerius.com.**
- Domain : groups_dir.cerius.com.
- Access Rights : ----rmcdr---r---
- Time to Live : 1:0:0
- Object Type : GROUP
- Group Flags :
- Group Members :
- ctg500g.cerius.com.

with the following members…

- **ctg500g#: nisgrpadm –l admin.cerius.com.**
- Group entry for "admin.cerius.com." group:
- Explicit members:
- **ctg500g.cerius.com.**
- No implicit members
- No recursive members
- No explicit nonmembers
- No implicit nonmembers
- No recursive nonmembers

Public key is set for the root domain

- **ctg500#: niscat –o cerius.com.**
- Object Name : cerius
- Owner : ctg500g.cerius.com.
- Group : admin.cerius.com.
- Domain : com.
- Access Rights : r---rmcdrmcdr---
- Time to Live : 24:0:0
- **Object Type : DIRECTORY**
- **Name : 'cerius.com.'**
- Type : NIS
- Master Server :
- Name : ctg500g.cerius.com.
- **Public Key : Diffie-Hellman (196 bits)**
- Universal addresses (5)
- [1] - udp, inet, 192.168.1.114.0.111
- [2] - tcp, inet, 192.168.1.114.0.111
- [3] - -, loopback, ctg500g.rpc
- [4] - -, loopback, ctg500g.rpc
- [5] - -, loopback, ctg500g.rpc
- Time to live : 12:0:0
- Default Access rights :

Public key is set for the org_dir object

- **ctg500#: niscat –o org_dir.cerius.com.**
- Object Name : org_dir
- Owner : ctg500g.cerius.com.
- Group : admin.cerius.com.
- Domain : cerius.com.
- Access Rights : r---rmcdrmcdr---
- Time to Live : 12:0:0
- **Object Type : DIRECTORY**
- **Name : 'org_dir.cerius.com.'**
- Type : NIS
- Master Server :
- Name : ctg500g.cerius.com.
- **Public Key : Diffie-Hellman (196 bits)**
- Universal addresses (5)
- [1] - udp, inet, 192.168.1.114.0.111
- [2] - tcp, inet, 192.168.1.114.0.111
- [3] - -, loopback, ctg500g.rpc
- [4] - -, loopback, ctg500g.rpc
- [5] - -, loopback, ctg500g.rpc
- Time to live : 12:0:0
- Default Access rights :

Public key is set for the groups_dir object

- **ctg500#: niscat –o groups_dir.cerius.com.**
- Object Name : groups_dir
- Owner : ctg500g.cerius.com.
- Group : admin.cerius.com.
- Domain : cerius.com.
- Access Rights : r---rmcdrmcdr---
- Time to Live : 12:0:0
- **Object Type : DIRECTORY**
- **Name : 'groups_dir.cerius.com.'**
- Type : NIS
- Master Server :
- Name : ctg500g.cerius.com.
- **Public Key : Diffie-Hellman (196 bits)**
- Universal addresses (5)
- [1] - udp, inet, 192.168.1.114.0.111
- [2] - tcp, inet, 192.168.1.114.0.111
- [3] - -, loopback, ctg500g.rpc
- [4] - -, loopback, ctg500g.rpc
- [5] - -, loopback, ctg500g.rpc
- Time to live : 12:0:0
- Default Access rights :

Step #2: Populate the NIS+ tables on the master root server

- **ctg500g#: mkdir /nisp-files**
- **ctg500g#: cp group hosts mail/aliases netgroup networks passwd protocols rpc services TIMEZONE /nisp-files**
- **(may also include auto_master and auto_home)**

Edit *all copied files* to include info that is to be part of the NIS+ namespace

- ctg500g#:**vi /nisp-files/passwd**
- *Remove all system users, the file now looks like this:*
- opc_op:*:777:77:OpC default operator:/home/opc_op:/usr/bin/ksh
- smokey:v4sL5vFQjQWQ2:4009:20:,,,:/home/smokey:/usr/bin/sh
- bvaught:D5QPwERnJ5fWE:4006:20:,,,:/home/bvaught:/usr/bin/sh
- jsmith:O5iekxm8SmhAQ:4010:20:,,,:/home/jsmith:/usr/bin/sh
- jrice:e58pcdIVHD8uM:4004:20:,,,:/home/jrice:/usr/bin/sh
- brankin:.6G.c23hKwGDY:4005:20:,,,:/home/brankin:/usr/bin/sh
- alinker:P7XbAX7UOxGK6:4011:20:,,,:/home/alinker:/usr/bin/sh
- bobr:f7IUHw4MwuK0k:4003:20:,,,:/home/bobr:/usr/bin/sh

Populate the tables using the edited files

- ctg500g#: **nispopulate -F -p /nisp-files**
- NIS+ domain name : cerius.com.
- Directory Path : /nisp-files
- Is this information correct? (type 'y' to accept, 'n' to change) **y**
- This script will populate the standard NIS+ tables for domain
- cerius.com. from the files in /nisp-files:
- auto_master auto_home ethers group hosts networks passwd protocols services rpc
- netmasks bootparams netgroup aliases
- **WARNING: Interrupting this script after choosing to continue
- may leave the tables only partially populated. This script does
- not do any automatic recovery or cleanup.
- Do you want to continue? (type 'y' to continue, 'n' to exit this script) **y**

Populating the NIS+ credential table for domain cerius.com.
from hosts table.
dumping hosts table...
loading credential table...
The credential table for domain cerius.com. has been populated.
The password used will be nisplus.
populating networks table from file /nisp-files/networks...
networks table done.
populating passwd table from file /nisp-files/passwd...
passwd table done.
Populating the NIS+ credential table for domain cerius.com.
from passwd table.
dumping passwd table...
loading credential table...
The credential table for domain cerius.com. has been populated.
The password used will be nisplus.
populating protocols table from file /nisp-files/protocols...
protocols table done.
populating services table from file /nisp-files/services...
services table done.
populating rpc table from file /nisp-files/rpc...
rpc table done.

**WARNING: file /nisp-files/netmasks does not exist!
netmasks table will not be loaded.
**WARNING: file /nisp-files/bootparams does not exist!
bootparams table will not be loaded.
populating netgroup table from file /nisp-files/netgroup...
netgroup table done.
populating mail_aliases table from file /nisp-files/aliases...
mail_aliases table done.
Credentials have been added for the entries in the hosts and passwd table(s). Each entry was given a defaultnetwork password (also known as a Secure-RPC password).

This password is:

nisplus

Use this password when the nisclient script requests the network password.
nispopulate failed to populate the following tables:
auto_master auto_home ethers netmasks bootparams

View the entries

- ctg500g#: **niscat hosts.org_dir passwd.org_dir**
- ctg700 ctg700 192.168.1.124
- ctg700 kerberos 192.168.1.124
- ctg701 ctg701 192.168.1.125
- ctg701 replica 192.168.1.125
- ctg500g ctg500g 192.168.1.114
- ctg500g rootmstr 192.168.1.114
- opc_op:*:777:77:OpC default operator:/home/opc_op:/usr/bin/ksh:
- smokey:v4sL5vFQjQWQ2:4009:20:,,,:/home/smokey:/usr/bin/sh:
- bvaught:D5QPwERnJ5fWE:4006:20:,,,:/home/bvaught:/usr/bin/sh:
- jsmith:O5iekxm8SmhAQ:4010:20:,,,:/home/jsmith:/usr/bin/sh:
- jrice:e58pcdIVHD8uM:4004:20:,,,:/home/jrice:/usr/bin/sh:
- brankin:.6G.c23hKwGDY:4005:20:,,,:/home/brankin:/usr/bin/sh:
- alinker:P7XbAX7UOxGK6:4011:20:,,,:/home/alinker:/usr/bin/sh:
- bobr:f7IUHw4MwuK0k:4003:20:,,,:/home/bobr:/usr/bin/sh:
- bobby:s7NQ.k2CW4ZIc:4100:20:,,,:/home/bobby:/usr/bin/sh:

NIS_DOMAIN added

- ctg500g#: **more /etc/rc.config.d/namesvrs**
- NIS_MASTER_SERVER=0
- NIS_SLAVE_SERVER=0
- NIS_CLIENT=0
- NISPLUS_SERVER=1
- NISPLUS_CLIENT=1
- **NIS_DOMAIN=cerius.com**
- MAX_NISCHECKS=2
- EMULYP=""

Step #3: Add non-root user to admin group

- **ctg500g#: nisgrpadm –a admin.cerius.com. jrice.cerius.com.**
- Added "jrice.cerius.com." to group "admin.cerius.com."
- **ctg500#: nisgrpadm –l admin.cerius.com.**
- Group entry for "admin.cerius.com." group:
- Explicit members:
- **ctg500g.cerius.com.**
- **jrice.cerius.com.**
- No implicit members
- No recursive members
- No explicit nonmembers
- No implicit nonmembers
- No recursive nonmembers

Step #4: Setup checkpointing on the root master server

- **ctg500g#: nisping –Ca**
  - Checkpointing replicas serving directory cerius.com. :
  - Master server is ctg500g.cerius.com.
  - Last update occurred at Thu Nov 8 09:38:00 2001
  - Master server is ctg500g.cerius.com.
  - checkpoint scheduled on ctg500g.cerius.com..
- **00 04 * * * /usr/lib/nis/nisping -Ca**

Step #5: Reboot

- 3 daemons:
  - /usr/sbin/rpc.nisd
  - /usr/sbin/nis_cachemgr
  - /usr/sbin/rpc.nispasswdd
- ctg500g#: **grep nisd /var/adm/syslog/syslog.log**
  - Nov 8 09:57:47 ctg500g syslog: rpc.nisd: cannot set credential cache size
  - Nov 8 09:57:47 ctg500g nisd[727]: NIS+ service started.

Replica Server:

Copy of Information. Runs NIS+ Server Software.

Provides increased performance & reliability.

Create a root replica server

- NIS+ commands used:
  - nisgrep
  - nisclient
  - nisdefaults
  - nisstat
  - nisshowcache

Step #1a: Update the PATH variable:

- **ctg701g#: vi /etc/PATH**
- /usr/bin:/usr/ccs/bin:/usr/contrib/bin:/opt/nettladm/bin:/opt/fc/bin:/opt/fcms/bin:/opt/upgrade/bin:/opt/pd/bin:/usr/bin/X11:/usr/contrib/bin/X11:/opt/hparray/bin:/opt/resmon/bin:/opt/perf/bin:/opt/ignite/bin:/opt/OV/bin/OpC:/opt/scr/bin:/opt/mx/bin://opt/perl/bin:/usr/sbin/diag/contrib:/opt/pred/bin**:/usr/lib/nis**
- Relogin or: export PATH=$PATH:/usr/lib/nis

Step #1b: Change startup scripts

The replica server must first be a client of the root master server

- **ctg701g#: vi /etc/rc.config.d/namesvrs**
- NIS_MASTER_SERVER=0
- NIS_SLAVE_SERVER=0
- NIS_CLIENT=0
- NISPLUS_SERVER=0
- **NISPLUS_CLIENT=1**
- NIS_DOMAIN=""

Check credentials for replica server (on the root master server)

- **ctg500g#: nisgrep ctg701 cred.org_dir.cerius.com.**

ctg701.cerius.com.:DES:unix.ctg701@cerius.com:ab7e8f0f7c07db6ae799a4fef706ae61948989303
cd6e3a1::f3d001b49af95b88a81574ce53a9ee0957d63d6a6b0b609f49ede68b9d5829a0

This would already be added if ctg701 was in the hosts file used to populate the tables.

Step #1c: Create separate Logical Volume for NIS+ namespace

- ctg701#: lvcreate -L 100 -n nis vg00
- ctg701#: newfs -F vxfs /dev/vg00/rnis
- ctg701#: mkdir /var/nis
- ctg701#: vi /etc/fstab
  - /dev/vg00/nis /var/nis vxfs delaylog 0 2
- ctg701#: mountall or manual mount

Configure as a NIS+ client

- **ctg701#: /usr/bin/domainname cerius.com.**
- **ctg701#: nisclient -i -h ctg500g *-d cerius.com.***
  - Initializing client ctg701 for domain "cerius.com.".
  - Once initialization is done, you will need to reboot your machine.
  - Do you want to continue? (type 'y' to continue, 'n' to exit this script) **y**

setting up domain information "cerius.com."...
setting up the name service switch information...
mv: /var/nis/NIS_COLD_START: cannot access: No such file or directory
At the prompt below, type the network password (also known
as the Secure-RPC password) that you obtained either
from your administrator or from running the nispopulate script.
Please enter the Secure-RPC password for root: (nisplus)
Please enter the login password for root: (root99)
Your network password has been changed to your login one.
Your network and login passwords are now the same.
Client initialization completed!!
Please ***reboot*** your machine for changes to take effect.

A client has these 2 files

- ctg701#: ll /var/nis
- -rw-r--r-- 1 root sys 308 Nov 8 10:13 NIS_COLD_START
- -rw-r--r-- 1 root sys 8192 Nov 8 10:13 NIS_SHARED_DIRCACHE

A client runs this daemon

- /usr/sbin/nis_cachemgr

nisdefaults command

- **ctg701#: nisdefaults**
  - Principal Name : ctg701.cerius.com.
  - Domain Name : cerius.com.
  - Host Name : ctg701.cerius.com.
  - Group Name :
  - Access Rights : ----rmcdr---r---
  - Time to live : 12:00:00
  - Search Path : cerius.com.

Configure as a root replica

- *The rpc.nisd daemon must be running in order for the root master server to communicate with the root replica server. Since it is not yet a server, you must start it manually.*
- **ctg701#: rpc.nisd**

Create the replica server *on the master root server*

- **ctg500g#: nisserver -R -h ctg701**
- This script sets up an NIS+ replica server for domain
- cerius.com.
- Domain name : cerius.com.
- NIS+ server : ctg701
- Is this information correct? (type 'y' to accept, 'n' to change) **y**
- This script will set up machine "ctg701" as an NIS+
- replica server for domain cerius.com. without NIS compatibility.
- The NIS+ server daemon, rpc.nisd, must be running on ctg701
- with the proper options to serve this domain.
- Do you want to continue? (type 'y' to continue, 'n' to exit this script) **y**
- Added "ctg701.cerius.com." to group "admin.cerius.com.".
- The system ctg701 is now configured as a replica server for
- domain cerius.com..
- The NIS+ server daemon, rpc.nisd, must be running on ctg701
- with the proper options to serve this domain.

Change the startup script

- **ctg701#: vi /etc/rc.config.d/namesvrs**
- NIS_MASTER_SERVER=0
- NIS_SLAVE_SERVER=0
- NIS_CLIENT=0
- **NISPLUS_SERVER=1**
- NISPLUS_CLIENT=1
- NIS_DOMAIN=""

Now that it is a nameserver….

- **ctg701#: ll /var/nis**
  - NIS_COLD_START
  - NIS_SHARED_DIRCACHE
  - **drwx------ 2 root root 1024 Nov 8 10:22 ctg701**
  - **-rw------- 1 root root 65537 Nov 8 10:22 ctg701.log**

Force an update

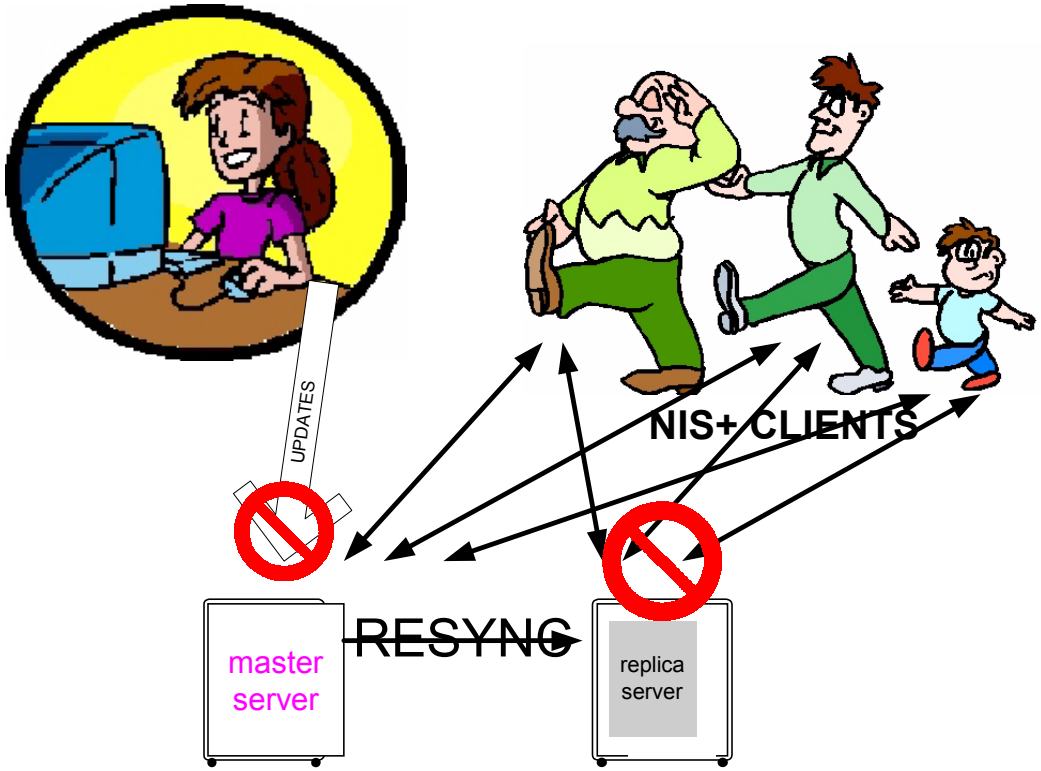
- ***Before*:** **ctg500g#: ll /var/nis**
  - NIS_COLD_START
  - NIS_SHARED_DIRCACHE
  - drwxr--r-- 2 root sys ctg500g
  - -rw-r--r-- 1 root sys ctg500g.dict
  - ***-rw-r--r-- 1 root root ctg500g.dict.log***
  - -rw------- 1 root sys ctg500g.log
- **ctg500g#: nisping –Ca**
- ***After*:** **ctg500g#: ll /var/nis**
  - NIS_COLD_START
  - NIS_SHARED_DIRCACHE
  - drwxr--r-- 2 root sys ctg500g
  - -rw-r--r-- 1 root root ctg500g.dict
  - -rw------- 1 root sys ctg500g.log

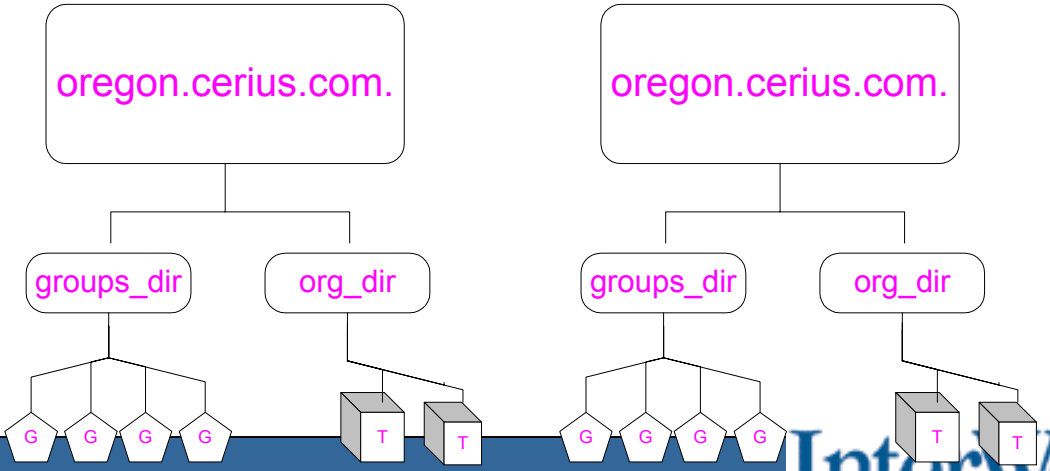
Resync:

A resync is a complete download from the master to the replica.

During this time updates are ***not*** accepted on the master.

During this time, reads are only accepted by the master. The replica is not accessible.





Msgs in syslog from forced update

- Nov 8 17:34:36 ctg500g nisd[4829]: nis_dump_svc: **sending full dump of cerius.com. to ctg701.cerius.com.**
- Nov 8 17:34:36 ctg500g nisd[4829]: nis_dump_svc: **good dump of cerius.com., 2 total objects.**
- Nov 8 17:34:39 ctg500g nisd[4829]: nis_dump_svc: Finish handshake returned RPC: Timed out
- Nov 8 17:34:48 ctg500g nisd[4832]: nis_dump_svc: **sending full dump of groups_dir.cerius.com. to ctg701.cerius.com.**
- Nov 8 17:34:48 ctg500g nisd[4832]: nis_dump_svc: **good dump of groups_dir.cerius.com., 1 total objects.**
- Nov 8 17:34:51 ctg500g nisd[4832]: nis_dump_svc: Finish handshake returned RPC:

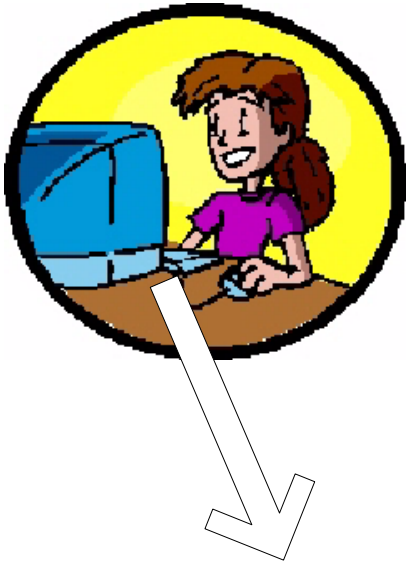
Updates:

Written to batch file.

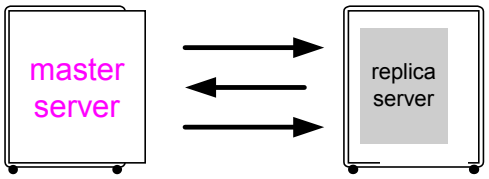
Apx. every 2 minutes, the server checks to see if there are any updates.

The batch file is placed in a transaction log with a timestamp.

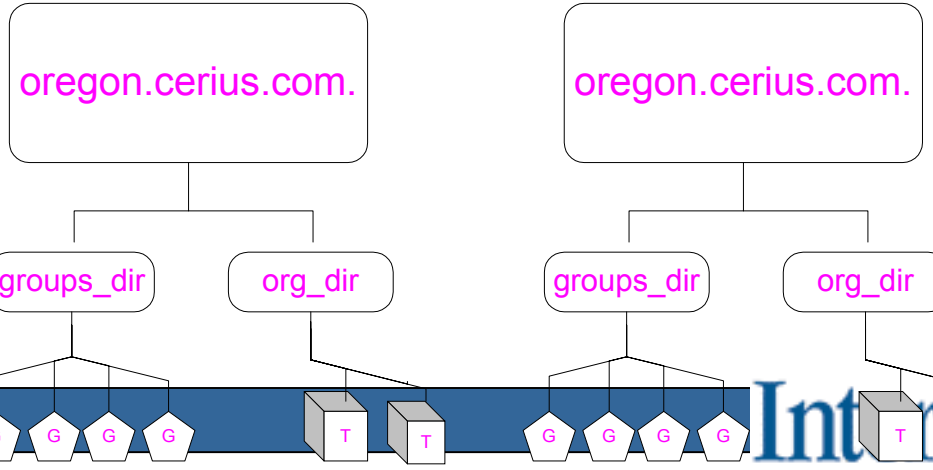
When all replicas are updated, the log is cleared.



Master: Hey, I've got an update. When was your last timestamp?
Replica: Timestamp2
Master: Here comes an update!



Transfers are encrypted



These messages in syslog indicate time is not synchronized between servers

- Nov 9 11:17:43 ctg500g nisd[737]: _svcauth_des: **timestamp is earlier than the one previously seen from unix.ctg500g@cerius.com**
- Nov 9 11:19:06 ctg500g nisd[737]: _svcauth_des: **timestamp is earlier than the one previously seen from unix.ctg701@cerius.com**

ctg500g#: nisstat –H ctg701

```
Statistics for domain cerius.com. :
Statistics from server : ctg701.cerius.com.
Stat 'root server' = 'ON'
Stat 'NIS compat mode' = 'OFF'
Stat 'security level' = '2'
Stat 'serves directories':
        cerius.com.
        groups_dir.cerius.com.
Stat 'Operation Statistics':
        OP=FINDDIR:C=11:E=0:T=542
        OP=STATUS:C=3:E=0:T=588
        OP=CPTIME:C=2:E=0:T=180
        OP=CHECKPOINT:C=1:E=0:T=153
        OP=PING:C=3:E=0:T=30478
        OP=SERVSTATE:C=1:E=0:T=266
Stat 'directory cache' = 'C=4:H=0:M=4:HR=0%'
Stat 'group cache' = 'C=0:H=0:M=0:HR=100%'
Stat 'static storage' = '4368'
Stat 'dynamic storage' = '1075150848'
Stat 'up since' = 'up 0D, 00:23:04'
```

ctg500g#: nisshowcache -v | more

Cache header:

vers: 1

mgr_uaddr: \000\000\020$

cache entries: 3

filesize: 8192 used: 1632 free: 6560

Cold Start Directory:

Name : 'cerius.com.'

Type : NIS

Master Server :

Name : ctg500g.cerius.com.

Public Key : Diffie-Hellman (196 bits)

Universal addresses (5)

[1] - udp, inet, 192.168.1.114.0.111

[2] - tcp, inet, 192.168.1.114.0.111

[3] - -, loopback, ctg500g.rpc

[4] - -, loopback, ctg500g.rpc

[5] - -, loopback, ctg500g.rpc

Replicate :

Name : ctg701.cerius.com.

Public Key : Diffie-Hellman (196 bits)

Universal addresses (2)

[1] - udp, inet, 192.168.1.125.0.111

[2] - tcp, inet, 192.168.1.125.0.111

Time to live : 11:55:13

Default Access rights :

NisDirCacheEntry[1]:

Name : 'org_dir.cerius.com.'

Type : NIS

Master Server :

Name : ctg500g.cerius.com.
Public Key : Diffie-Hellman (196 bits)
Universal addresses (5)
[1] - udp, inet, 192.168.1.114.0.111
[2] - tcp, inet, 192.168.1.114.0.111
[3] - -, loopback, ctg500g.rpc
[4] - -, loopback, ctg500g.rpc
[5] - -, loopback, ctg500g.rpc

Replicate :

Name : ctg701.cerius.com.
Public Key : Diffie-Hellman (196 bits)
Universal addresses (2)
[1] - udp, inet, 192.168.1.125.0.111
[2] - tcp, inet, 192.168.1.125.0.111

Time to live : 11:55:16

Default Access rights :

NisDirCacheEntry[2]:

Name : 'groups_dir.cerius.com.'

Type : NIS

Master Server :

Name : ctg500g.cerius.com.
Public Key : Diffie-Hellman (196 bits)
Universal addresses (5)
[1] - udp, inet, 192.168.1.114.0.111
[2] - tcp, inet, 192.168.1.114.0.111
[3] - -, loopback, ctg500g.rpc
[4] - -, loopback, ctg500g.rpc
[5] - -, loopback, ctg500g.rpc

Replicate :

Name : ctg701.cerius.com.
Public Key : Diffie-Hellman (196 bits)
Universal addresses (2)
[1] - udp, inet, 192.168.1.125.0.111
[2] - tcp, inet, 192.168.1.125.0.111

Time to live : 11:55:20

Default Access rights :

Edit the /etc files to contain only the entries not found in NIS+

- **ctg701#: vipw /etc/passwd**
- *Edit the file to contain only the system entries:*
- root:LU9yvl84sLVMM:0:3::/root:/sbin/sh
- daemon:*:1:5::/:/sbin/sh
- bin:*:2:2::/usr/bin:/sbin/sh
- sys:*:3:3::/:
- adm:*:4:4::/var/adm:/sbin/sh
- uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
- lp:*:9:7::/var/spool/lp:/sbin/sh
- nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
- hpdb:*:27:1:ALLBASE:/:/sbin/sh
- nobody:*:-2:-2::/:
- www:*:30:1::/:
- webadmin:*:40:1::/usr/obam/server/nologindir:/usr/bin/false
- smbnull:*:101:101:DO NOT USE OR DELETE - needed by Samba:/home/smbnull:/sbin/sh

This is the opposite of the files edited earlier

Test…

- **ctg701#: telnet ctg701**
  - login: **user01**
  - Password: (user01)
  - Password does not decrypt secret key for unix.5001@cerius.com.

That's the UID for user01

Each user should run …

ctg701: nisclient –u

At the prompt below, type the network password (also known
as the Secure-RPC password) that you obtained either
from your administrator or from running the nispopulate script.
Please enter the Secure-RPC password for **user01**: **(nisplus)**
Please enter the login password for **user01**: (unix password – **user01**)
Your network password has been changed to your login one.
Your network and login passwords are now the same.

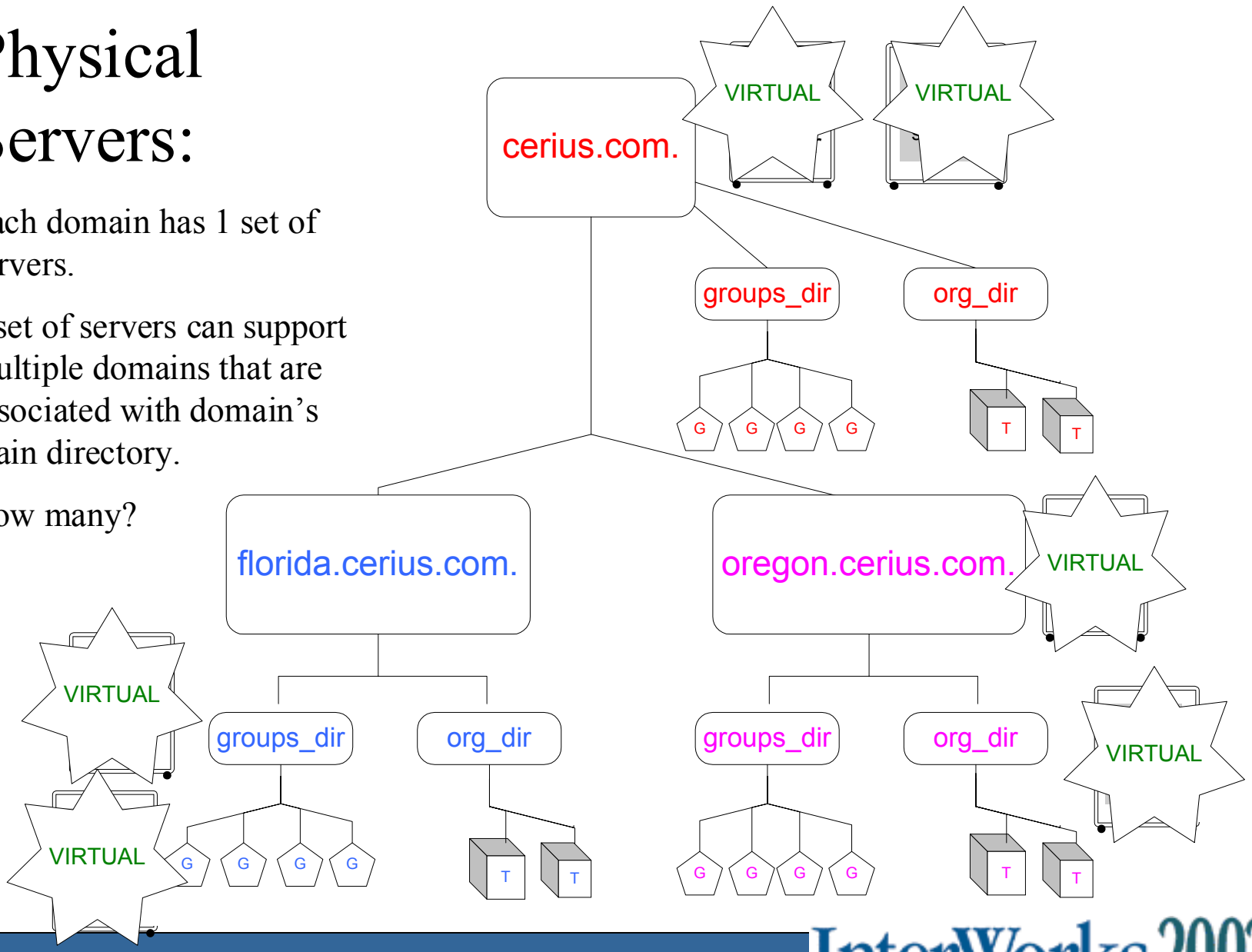
Physical Servers:

Each domain has 1 set of servers.

1 set of servers can support multiple domains that are associated with domain's main directory.

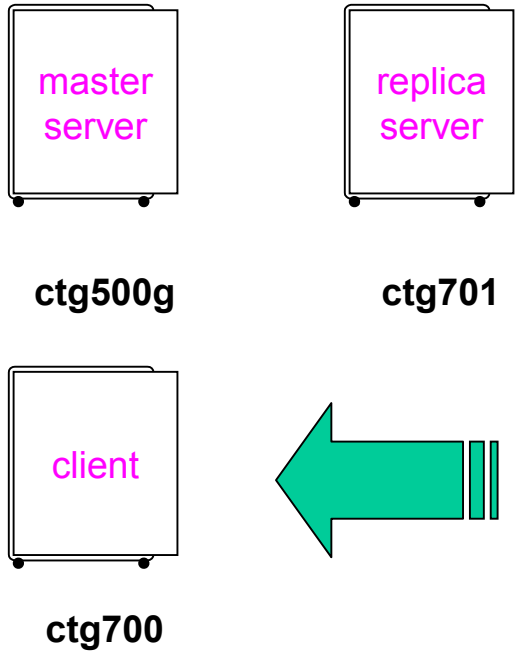
How many?

2



Add client only host

- Update PATH variable
- Change startup script
- Check credential on master or replica
- **ctg700#: nisclient -i -h ctg500g**
- Don’t need separate Logical Volume for /var/nis
- Edit /etc files to remove all NIS+ entries
- Reboot

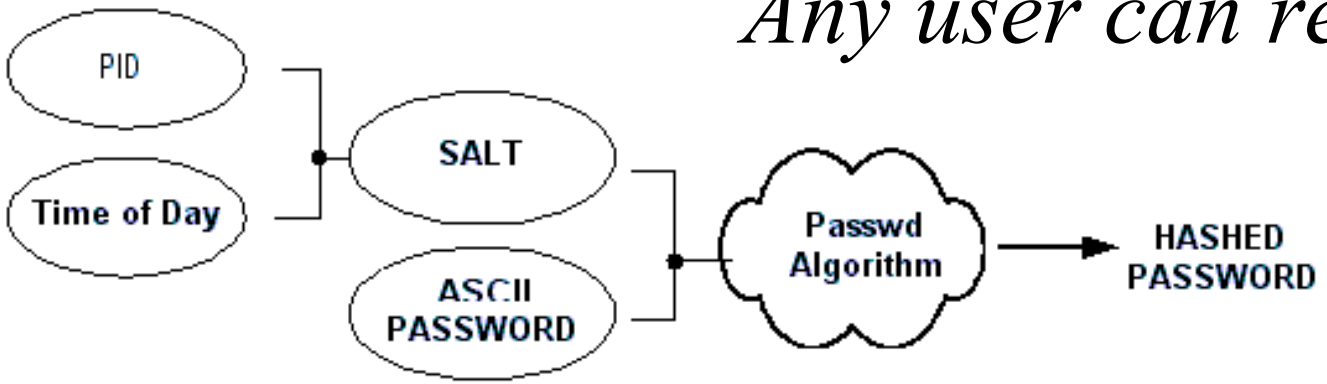


Trusted System

- NIS does not support the trusted system
- NIS+ is supported
- Why a trusted system?

The hashed password

Any user can read these



root:**dUusSnahft0NA**:0:3::/root:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico

vking:**5Q**oJE01/Hhxiw
wwong:TQRfi&sKYx.jc
bobr:HRgB7ju2XPZcw
jrice:VPGPXTvx3xCgw
brankin:rNa/Z2sa4ls92
smokey:OU3enGecqU/2M
jsmith:49FL9A6LxVxTc

crack

```
./Reporter
----passwords cracked as of Fri Dec  1 19:52:01 PST 2000
971920189:Guessed bvaught [kitty],, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],,, [/etc/passwd /usr/bin/sh]
971920189:Guessed bvaught [kitty],,, [/etc/passwd /usr/bin/sh]
971921701:Guessed brankin [5ing],,, [/etc/passwd /usr/bin/sh]
971921701:Guessed brankin [5ing],,, [/etc/passwd /usr/bin/sh]
```

Crack does not decrypt, it compares

The passwd.org_dir Table

niscat -h passwd.org_dir

opc_op:*:777:77:OpC default operator:/home/opc_op:/usr/bin/ksh:
smokey:v4sL5vFQjQWQ2:4009:20:,,,:/home/smokey:/usr/bin/sh:
bvaught:D5QPwERnJ5fWE:4006:20:,,,:/home/bvaught:/usr/bin/sh:
jsmith:O5iekxm8SmhAQ:4010:20:,,,:/home/jsmith:/usr/bin/sh:
jrice:e58pcdIVHD8uM:4004:20:,,,:/home/jrice:/usr/bin/sh:
brankin:.6G.c23hKwGDY:4005:20:,,,:/home/brankin:/usr/bin/sh:
alinker:P7XbAX7UOxGK6:4011:20:,,,:/home/alinker:/usr/bin/sh:
user01:E9npNCrXrC7iw:5001:102:,,,:/home/user01:/usr/bin/sh:

Can any user read these?

NIS+ Table Access Rights

(niscat -o passwd.org_dir)

Object Name : passwd
Owner : ctg500g.cerius.com.
Group : admin.cerius.com.
Domain : org_dir.cerius.com.
Access Rights : **----rmcdrmcdr---**
Time to Live : 12:0:0
Object Type : TABLE
Table Type : passwd_tbl
Number of Columns : 8
Character Separator : :
Search Path :
Columns :

Nobody

Owner

Group

World

Read, write, modify, destroy

Table Entry Rights

[0] Name : name

Attributes : (SEARCHABLE, TEXTUAL DATA, CASE SENSITIVE)

Access Rights : r---r---r---r---

[1] Name : **passwd**

Attributes : (TEXTUAL DATA)

Access Rights : **----rm--r---r---**

Lab: Trusting the System

- Make sure the non-system entries have been removed from /etc/passwd (should have already been done).
- /usr/lbin/tsconvert
  - Unconvert: tsconvert -r
- How to tell: /usr/lbin/getprdef -r
  - (Don't rely on just the /tcb directory existing)
- Always logon as root while a valid root account is still open
- Change backup parameters to include /tcb
  - Double check for /var/nis also
- nisping -Ca

Trusted System
Shadowed Password File

```
root:u_name=root:u_id#0:\
        :u_pwd= dUusSnahft0NA:\
        :u_bootauth:u_auditid#0:\
        :u_auditflag#1:\
        :u_minchg#0:u_exp#15724800:u_succhg#1005438958:u_pw_expire_warning#604800:\
        :u_pswduser=root:u_suclog#1005438958:u_suctty=pts/ta:u_lock@:\
        :chkent:
```

Trusted System “database”

```
/tcb/files:
auth        devassign   ttys
#
/tcb/files/auth:
A       G       M       S       Y       e       k       q       v
B       H       N       T       Z       f       l       r       w
C       I       O       U       a       g       m       s       x
D       J       P       V       b       h       n       system  y
E       K       Q       W       c       i       o       t       z
F       L       R       X       d       j       p       u


/tcb/files/auth/a:
adm       alinker

/tcb/files/auth/b:
bin       bobr      brankin   bshaver   bvaught   bwalton
```

Hey, I can’t see the password now.

/tcb/files/auth/r/root

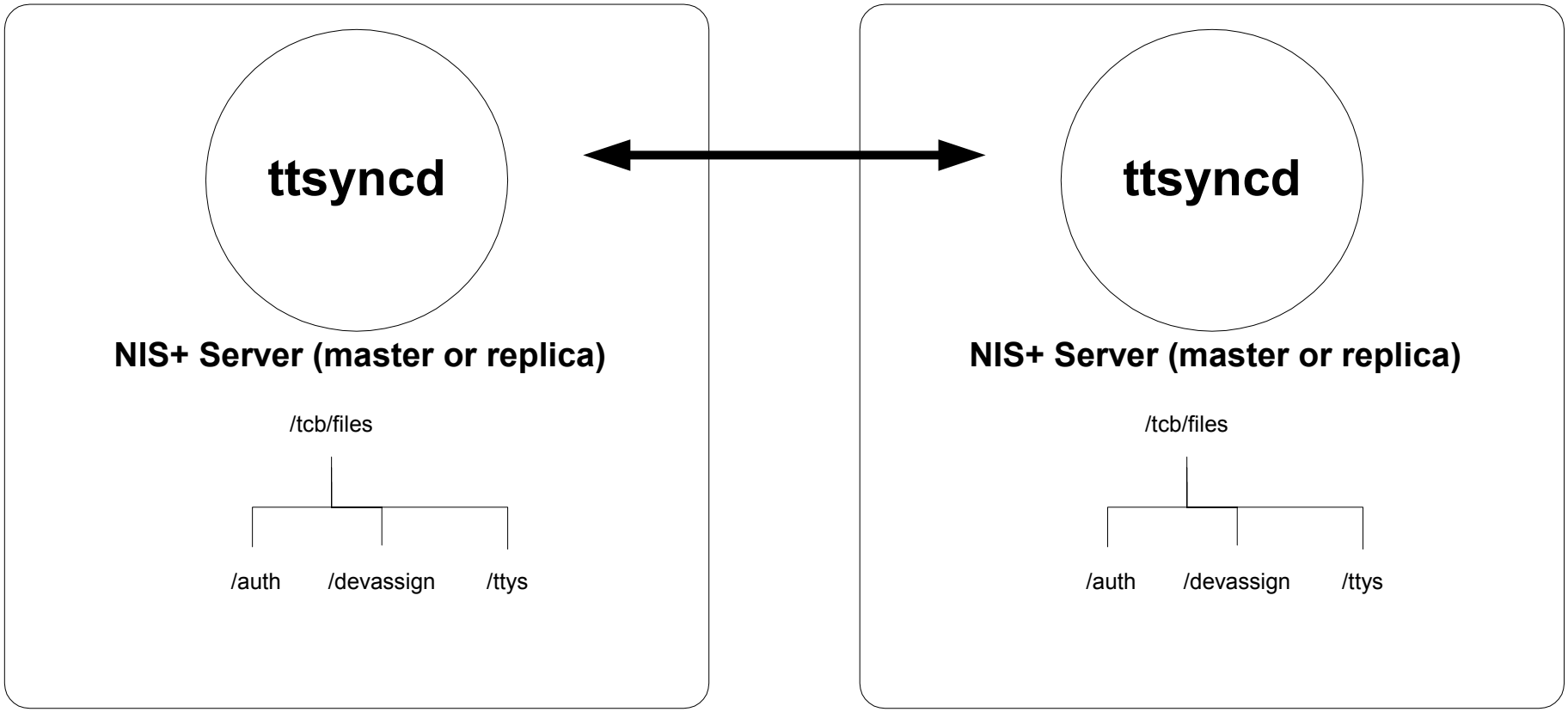
drwxrwx--x 3 root sys Nov 10 16:34 /tcb/files

When a system is converted to trusted:

- 1). The hashed password is removed from /etc/passwd and replaced with a “*”
- 2). The /tcb hierarchy is created
- 3). A separate file is created for each user within the hierarchy
- 4). Additional security features are now available

NIS+ and the Trusted System

- 1). NIS+ first
- 2). Convert system to trusted
- 3). ttsyncd must run on every NIS+ server
  - Edit /etc/rc.config.d/comsec
  - TTSYNCD=1



Added authorized login days and times. /tcb/files/auth/j/jsmith: **11:14**

Added authorized login days and times. /tcb/files/auth/j/jsmith: **11:17**

NIS+ user

- user01:00C3ACcI2Uv3c:5001:102:,,,:/home/user01:/usr/bin/sh:**11637::::::0**
- user02:BBk3YRtD203Wg:5002:107:,,,:/home/user02:/usr/bin/sh:

Once the system is trusted, the user's account will be expired and the user will be forced to change their password. (This has nothing to do with NIS+)

Remove “r” access to passwd column for “world”

- **nistbladm -u passwd=w-r passwd.org_dir**

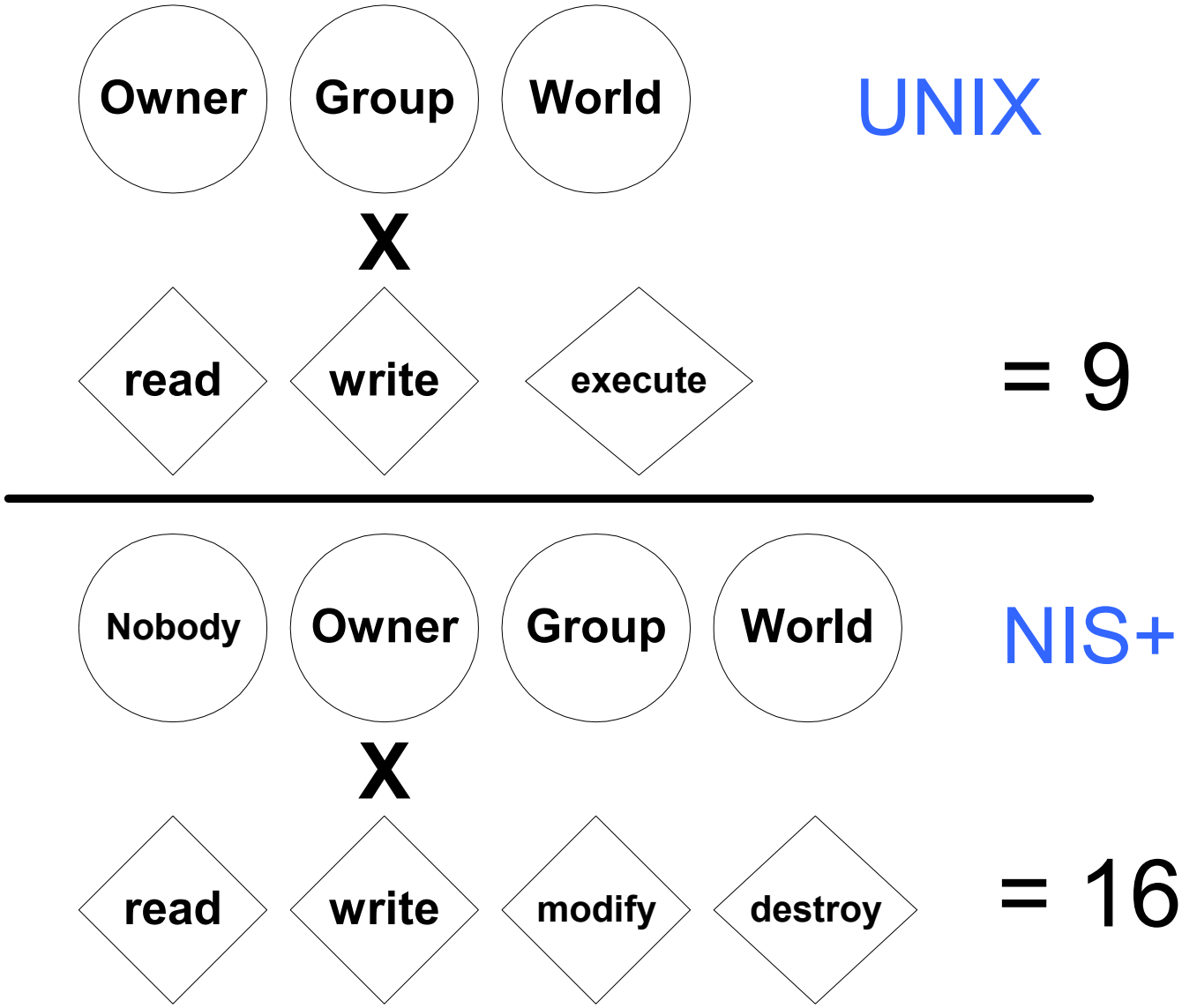
Trusting the system doesn’t fix the ability to view NIS+ passwords

```
Columns          :
     [0]   Name          : name
           Attributes    : (SEARCHABLE, TEXTUAL DATA, CASE SENSITIVE)
           Access Rights : r---r---r---r---
     [1]   Name          : passwd
           Attributes    : (TEXTUAL DATA)
           Access Rights : ----rm--r-------
```

Can the password still be read?

On ctg701, logon as the user: user01

niscat -h passwd.org_dir


Owner
Group
World
UNIX
X
read
write
execute
= 9
Nobody
Owner
Group
World
NIS+
X
read
write
modify
destroy
= 16

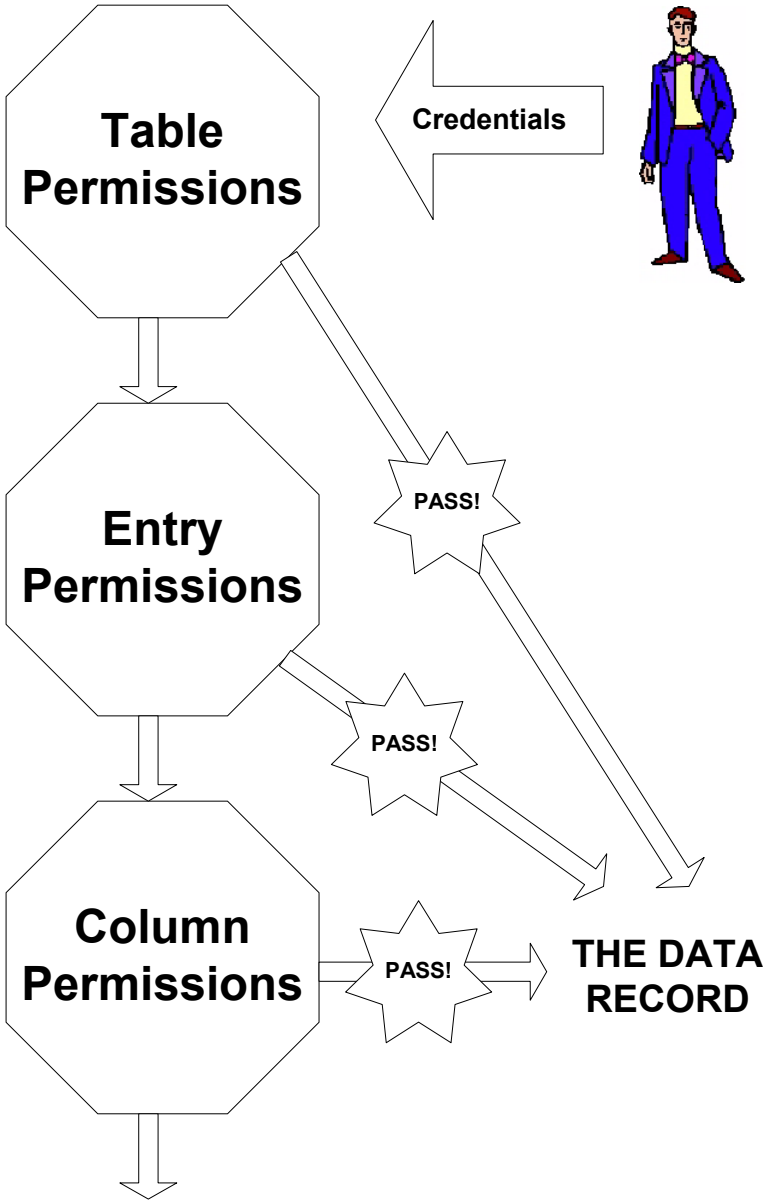


Table Permissions
Credentials
Entry Permissions
PASS!
PASS!
Column Permissions
PASS!
THE DATA RECORD
DENIED!

Change the Table Permissions

nischmod n=,og=rmcd,w= passwd.org_dir

check now: niscat -h passwd.org_dir

jrice:*NP*:4004:20:,,,:/home/jrice:/usr/bin/sh:*NP*
brankin:*NP*:4005:20:,,,:/home/brankin:/usr/bin/sh:*NP*
alinker:*NP*:4011:20:,,,:/home/alinker:/usr/bin/sh:*NP*
bobr:*NP*:4003:20:,,,:/home/bobr:/usr/bin/sh:*NP*
bobby:*NP*:4100:20:,,,:/home/bobby:/usr/bin/sh:*NP*
bshaver:*NP*:4013:20:,,,:/home/bshaver:/usr/bin/sh:*NP*
bwalton:*NP*:4012:20:,,,:/home/bwalton:/usr/bin/sh:*NP*
vking**:*NP*:**4002:20:,,,:/home/vking:/usr/bin/sh:*NP*
user01:**aos1wLnAUDG62**:5001:102:,,,:/home/user01:/usr/bin/sh:11637::::::0
user02:*NP*:5002:107:,,,:/home/user02:/usr/bin/sh:*NP*
user03:*NP*:5003:107:,,,:/home/user03:/usr/bin/sh:*NP*

user01 can only see their own password now

Additional Features of a Trusted System

- Protected Password Database
- Enhanced Login Configuration
- Auditing
- Terminal Restrictions
- Serial Port Restrictions
- Access Time Restrictions
- Password Generation
- Password Aging

Trusted System Hierarchy

/tcb/files/auth	Users, users, users!
/tcb/files/auth/system	System defaults
/tcb/files/devassign	Device assignments
/tcb/files/ttys	Port & terminal security

The Trusted system's system default file (/tcb/files/auth/system/default)

- Minimum time between password changes
- Maximum password length
- Expiration time of password
- Password lifetime
- Ability to pick passwords directly
- Ability to run password generator
- Password restriction checking is enabled/disabled
- Number of unsuccessful login tries allowed per user and per terminal
- Delay between unsuccessful login attempts on a terminal
- Total timeout for a login attempt on a terminal
- Auditing is enabled/disabled
- Null passwords allowed/disallowed
- Boot authentication
- Password expiration warning interval
- Account lock status
- Account expiration date
- Maximum time since last login until an account expiration warning

System Default File

```
default:\
        :d_name=default:\
        :d_boot_authenticated@:\
        :u_pwd=*:\
        :u_owner=root:u_auditflag#-1:\
        :u_minchg#0:u_maxlen#8:u_exp#15724800:\
        :u_life#16934400:\
        :u_pw_expire_warning#604800:u_pswduser=root:\
        :u_pickpw:u_genpwd:u_restrict@:u_nullpw@:\
        :u_genchars@:u_genletters:\
        :u_suclog#0:u_unsuclog#0:u_maxtries#3:u_lock:\
        :t_logdelay#2:t_maxtries#10:t_login_timeout#0:\
        :chkent:
```

@ = not allowed

followed by value

d	Default – System Wide, unless contained in user's file
u	User – Defaults for User Password Database
t	Terminal – Defaults for Terminal Control Database
v	Device – Defaults for Device Assignment Database

Password Selections

- Random Syllables: A pronounceable password made up of meaningless syllables
- Random Characters: An unpronounceable password made up of random characters from the character set
- Random Letters: An unpronounceable password made up of random letters from the alphabet
- User Supplied: A user-supplied password, subject to length and triviality restrictions

Name of Entry	**Quick Pick Letter & Description**
u_genpwd	g (Pronounceable password)
u_genchars	c (String of characters)
u_genletters	l (String of letters)
u_pickpw	p (Pick your password)

User's settings and the system defaults

- For the users file: Allow "p" and disallow "g"
- For the system file: Allow "g" and allow "c"

```
Do you want (choose one letter only):
        a string of characters generated (c) ?
        to pick your passwords (p) ?

Enter choice here: _
```

Adding a user

- Commands used:
  - modprpw
  - nistbladm
  - nisaddcred
- Only use useradd to create a non-NIS+ user.
  - System users (less than UID 100)

Example: Create new user named newuser5 with UID 7005

- **ctg500g#: /usr/lbin/modprpw –A –n cerius.com. –m uid=7005 newuser5**
  - The default password is displayed:
    - **aunoothi**

The /tcb/files/auth/n/newuser5 file was created. The password is in this file. An entry is added to the NIS+ password table with no password (-n option).

- **ctg500g#: nistbladm –m gid=20 shell=/usr/bin/sh home=/home/newuser5 [name=newuser5],passwd.org_dir.cerius.com.**

The password is added to the NIS+ password table entry.

Create local credentials

ctg500g#: nisaddcred –p 7005 –P
newuser5.cerius.com. local cerius.com.

Create DES credentials

ctg500g#: nisaddcred –p unix.7005@cerius.com -P
newuser5.cerius.com. des cerius.com.
login password? **aunoothi**

nisgrep newuser5 cred.org_dir.cerius.com.

- newuser5.cerius.com.:**LOCAL**:7005:20:
- newuser5.cerius.com.:**DES**:unix.7005@cerius.com:4f83108b80d8bae3e4cd3f04c54e8db5d31c199265fbf37a::428907e5a93833eda1e479d03d6b4cd93892d22e86ea34b57cb37f9be1d7855f

Create user's environment

- **ctg500g#: mkdir /home/newuser5**
- **ctg500g#: cp -R /etc/skel /home/newuser5**
- **ctg500g#: chown –R 7005:20 /home/newuser5**

Users: Changing Password

- First logon after conversion to NIS+: nisclient -u
- Logon after conversion to Trusted System: Forced to change user password
- User should use: nispasswd to change their password

NIS+ and the Trusted System user passwords

- The UNIX password is stored in the /tcb hierarchy
- The NIS+ password is stored in the passwd Table
- ttsyncd keeps the UNIX passwords synchronized
- NIS+ keeps the NIS+ passwords synchronized
- User must use nispasswd to keep the UNIX and NIS+ passwords the same

- **nispasswd does not read or modify the local password information stored in the**
- **/etc/passwd file**.

- When used to change a password, nispasswd prompts non-privileged users for
- their old password. It then prompts for the new password twice to forestall typing
- mistakes. When the old password is entered, nispasswd checks to see if it has
- aged sufficiently. If aging is insufficient, nispasswd terminates; see getpwent(3C)

- **The old password is used to decrypt the username's secret key**. If the password
- does not decrypt the secret key, nispasswd prompts for the old secure-RPC
- password. It uses this password to decrypt the secret key. If this fails, it gives the
- user one more chance. The old password is also used to ensure that the new
- password differs from the old by at least three characters. Assuming aging is
- sufficient, a check is made to ensure that the new password meets construction
- requirements described below. When the new password is entered a second
- time, the two copies of the new password are compared. If the two copies are
- not identical, the cycle of prompting for the new password is repeated twice.
- **The new password is used to re-encrypt the user's secret key. Hence, it also**
- **becomes their secure-RPC password.**
    - ***FROM: HP-UX 11i Version 1.5 Reference Volume 1, Section 1***

passwd vs. nispasswd

- For 10.30+, the commands nispasswd, yppasswd and passwd are integrated into the one command /usr/bin/passwd.
- So…. Using passwd is the same as using nispasswd (if not on 10.20)

Admin needs to change user's password

- Change the UNIX password:
  - passwd jsmith
- Change the NIS+ password:
  - newkey -u jsmith

From HP-UX Reference Volume 5:

newkey prompts for a password for the given username or hostname and then creates a new public/secret Diffie-Hellman 192 bit key pair for the user or host.
The secret key is encrypted with the given password. The key pair can be stored in the /etc/publickey file, the NIS publickey map, or the NIS+ ==cred.org_dir table.

Adding a new client (ctg800) (did not exist when NIS+ created)

- Add *new* entry to hosts table
- *Modify* entry in hosts table

Check Credentials for host named ctg800

- **Check Credentials**
- **ctg500g#: nisgrep ctg cred.org_dir.cerius.com.**
- **ctg500g.cerius.com**.:DES:unix.ctg500g@cerius.com:77faa98a1adf3f5438ce3c81ce8f497633f0299d5ce681fa::98c49755cd3e68473ab0e09e27766ec109b1a1bad8ef9f1bae447049789b28f7
- **ctg700.cerius.com**.:DES:unix.ctg700@cerius.com:2be7bcf45f30cef8ca92ccf0c0c16b2f840f04cc94abfd8e:3b3b4c20757f8fbbbdc4d3d00d577b34d6c621d4780560e1064c1a8844f58430
- **ctg701.cerius.com**.:DES:unix.ctg701@cerius.com:1a2a202b1018cc9cc671a5d5f6fdc79aa8b671752a7021f2:55eb9333d6f9d47d49573466b003d130c32c75babed3c14d4fe7cb5b82fc1fec

Check to see if the client (ctg800) is in the hosts table

- **ctg500g#: nisgrep ctg hosts.org_dir**
  - ctg700 ctg700 192.168.1.124
  - ctg700 kerberos 192.168.1.124
  - ctg701 ctg701 192.168.1.125
  - ctg701 replica 192.168.1.125
  - ctg500g ctg500g 192.168.1.114
  - ctg500g rootmstr 192.168.1.114

ctg500g#: niscat –o hosts.org_dir

Object Name : hosts
Owner : ctg500g.cerius.com.
Group : admin.cerius.com.
Domain : org_dir.cerius.com.
Access Rights : r---rmcdrmcdr---
Time to Live : 12:0:0
Object Type : TABLE
Table Type : **hosts_tbl**
Number of Columns : **4**
Character Separator :
Search Path :

But.. we need to know the name of the columns

Columns :
[0] Name : **cname**
Attributes : (SEARCHABLE, TEXTUAL DATA, CASE INSENSITIVE)
Access Rights : ----------
[1] Name : **name**
Attributes : (SEARCHABLE, TEXTUAL DATA, CASE INSENSITIVE)
Access Rights : ----------
[2] Name : **addr**
Attributes : (SEARCHABLE, TEXTUAL DATA, CASE INSENSITIVE)
Access Rights : ----------
[3] Name : **comment**
Attributes : (TEXTUAL DATA)
Access Rights : ----------

Add the entry

ctg500g#: nistbladm –a
[cname=ctg800,name=ctg800,addr=192.1
68.1.117,comment=],hosts.org_dir

Create DES credentials

ctg500g#: nisaddcred –p unix.ctg800@cerius.com
-P ctg800.cerius.com. des cerius.com.

You will be prompted for the root password on ctg800 (twice)
Continue with instructions already covered for adding a client.

Or…. Use niscat –h to see the column names!

- ctg500g#: **niscat –h hosts.org_dir**
- # **cname name addr comment**
- ctg700 ctg700 192.168.1.124
- ctg700 kerberos 192.168.1.124
- ctg701 ctg701 192.168.1.125
- ctg701 replica 192.168.1.125
- ctg500g ctg500g 192.168.1.114
- ctg500g rootmstr 192.168.1.114
- **ctg800 ctg800 192.168.1.117**

Modify entry

Your phone rings…. The network administrator gave you the wrong IP address for that host you just added! You have to change it.

ctg500g#: nistbladm –m addr=192.168.1.134[cname=ctg800],hosts.org_dir

Field to modify

New value

for this entry

in this table

ctg500g#: nistbladm –m addr=192.168.1.099[cname=ctg701],hosts.org_dir

can’t modify entry: Name/entry isn’t unique.

ctg500g#: niscat –h hosts.org_dir

cname name addr comment
ctg700 ctg700 192.168.1.124
ctg700 kerberos 192.168.1.124
ctg701 ctg701 192.168.1.125
ctg701 replica 192.168.1.125
ctg500g ctg500g 192.168.1.114
ctg500g rootmstr 192.168.1.114
ctg800 ctg800 192.168.1.134

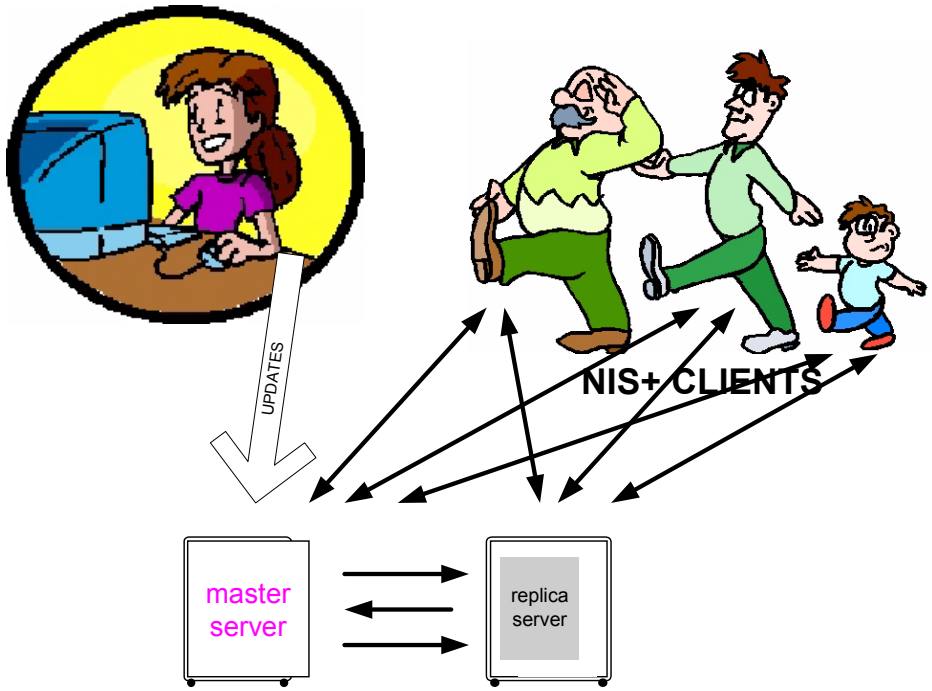
ctg500g#: nistbladm –m addr=192.168.1.099
[cname=ctg701,name=ctg701],hosts.org_dir

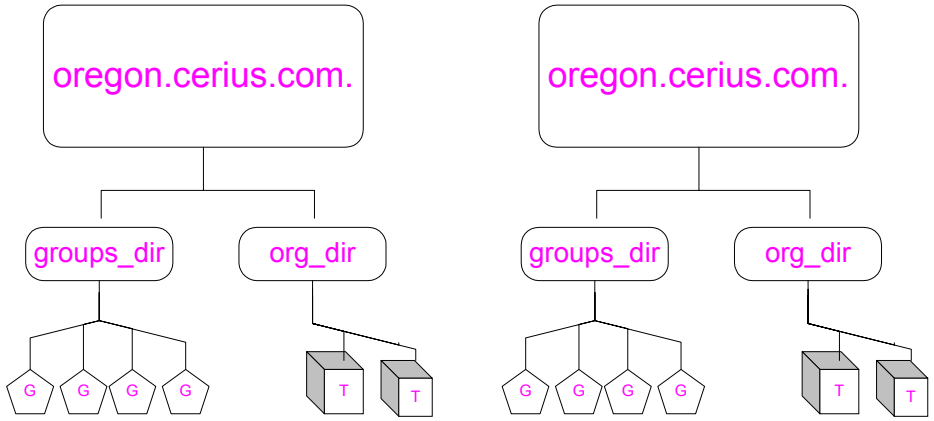
ctg500g#: nistbladm –m addr=192.168.1.099
[cname=ctg701,name=replica],hosts.org_dir

Must use enough column pairs to uniquely identify the record

Clients:

Client read requests can be handled by either the master or the replica.





NIS+ CLIENTS

What are these requests?

The /etc/nsswitch.conf File

NIS+

FILES

DNS

NIS

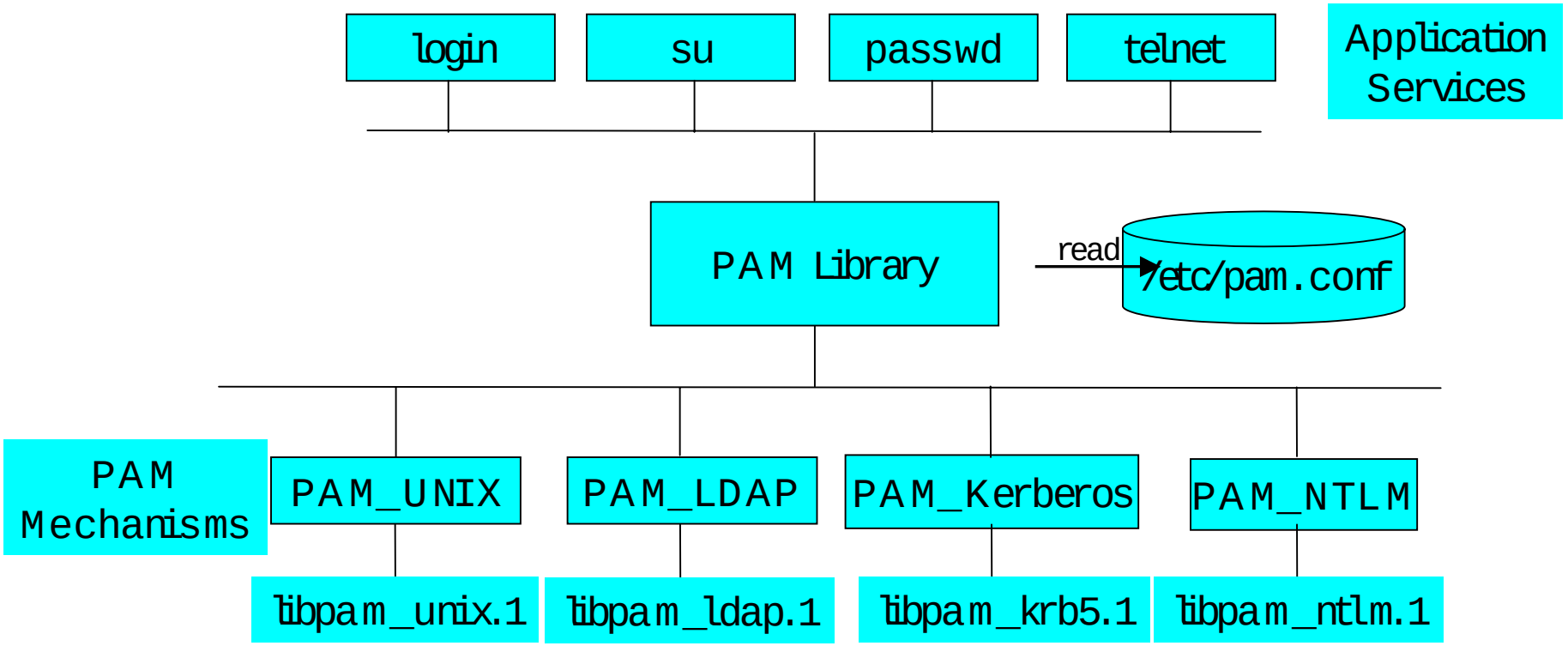
LDAP

Table

Table

HP-UX Authentication & PAM

login, passwd, ftp, rlogin, telnet, dtlogin, remsh (PAM and NSS)



Also: libpam_dce.1: DCE

Slide from: HP

HP-UX Commands that only use NSS

- finger
- grget
- groups
- id
- listusers
- logins
- logname
- ls
- newgrp
- pwget
- nsquery
- who
- whoami

NIS+ Summary

- NIS+ supported with a trusted system
- NIS+ encrypts transfers
- NIS+ more difficult to administer
- NIS+ supported on UNIX platforms
- Must: **All About Administering NIS+ (2nd Edition)** by Rick Ramsey
  Prentice Hall PTR; ISBN: 0133095762

Hope to see you….

- HP Booth 1:00 to 2:00
- Book signing from 2:00 to 3:00 today at the conference book store.
- “HP-UX 11i Security”