

Remote Desktop Service

An overview of CERN's remote access system



Authors

Petar Stojković

Pablo Martin Zamora

Mario Rey Regulez

Section

Device Provisioning and Productivity

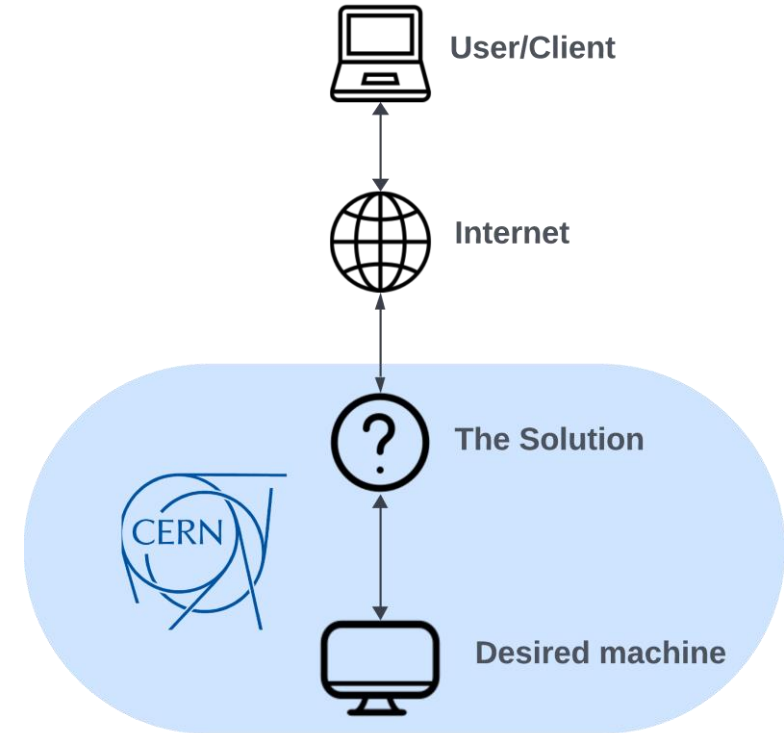
The Content

1. The Need for Remote Desktop Access at CERN
2. The challenges and the solution
3. Remote Desktop Gateway
4. The Simple Steps to Remote Access
5. User Engagement, System Capacity, and Usage History
6. RDP(ing) to Linux
7. Synchronization and its obstacles
8. Session Management
9. Debugger
10. Architecture



The Need for Remote Desktop Access at CERN

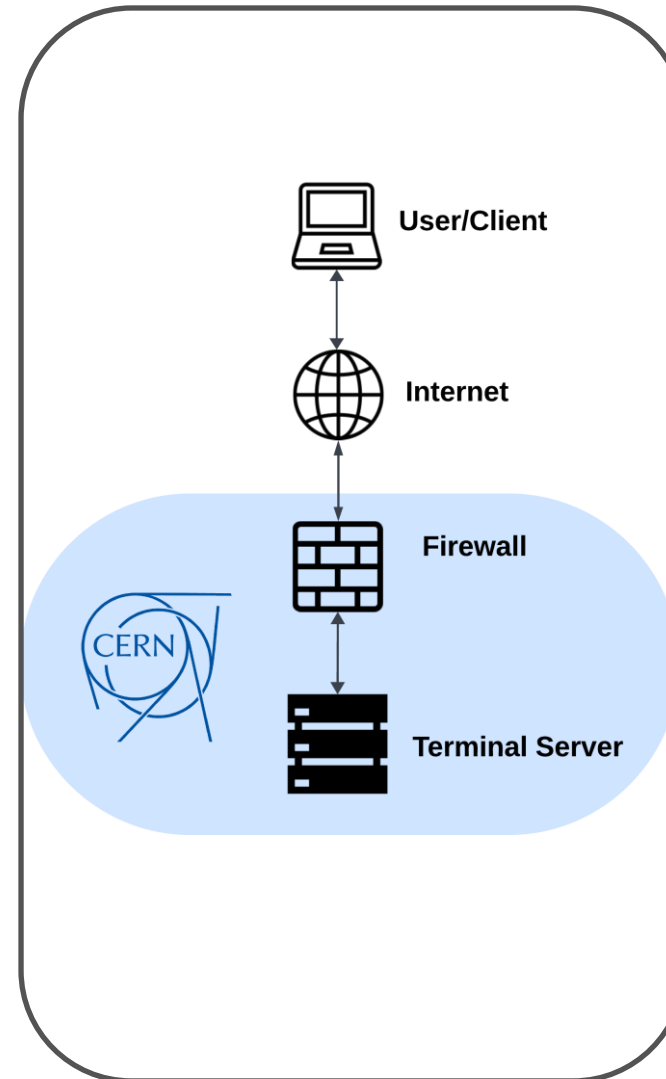
- CERN Windows Infrastructure
- Secure remoting outside of the CERN network
- **RDP** vs **VPN**
- Why not VPN?
- Security and granularity



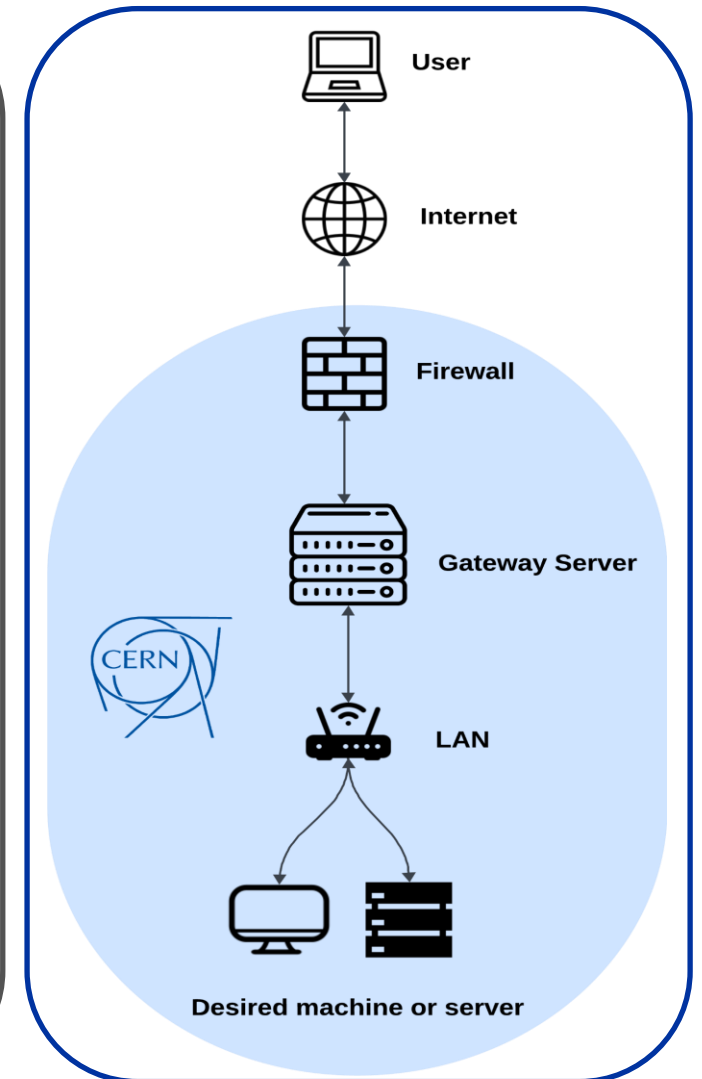
The Need for Remote Desktop Access at CERN

- Two big use cases of remote desktop access
 - Remote Desktop Gateway
 - Terminal Servers
- What is a Gateway Server?
- Remote Desktop Gateway
 - Standard Microsoft Tools + self-service

Terminal server



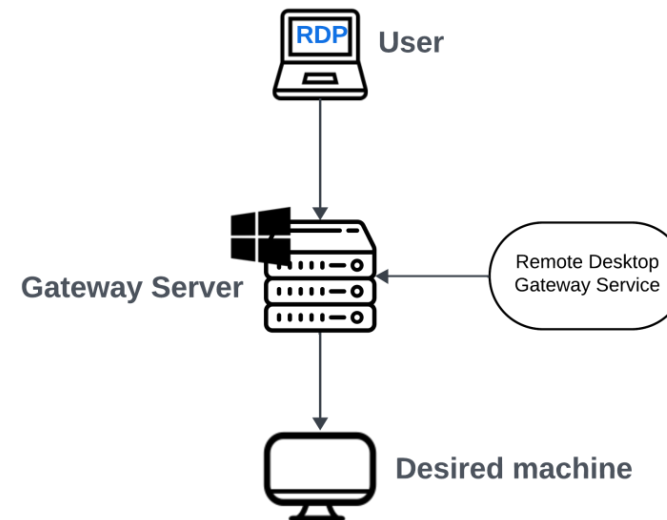
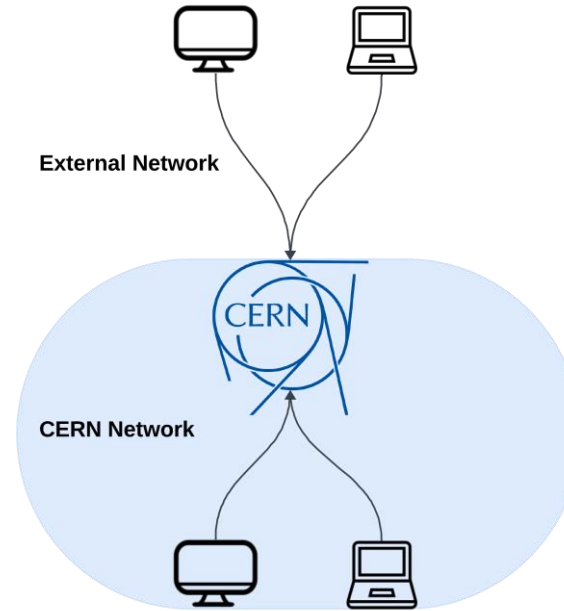
Gateway Server



The Challenges

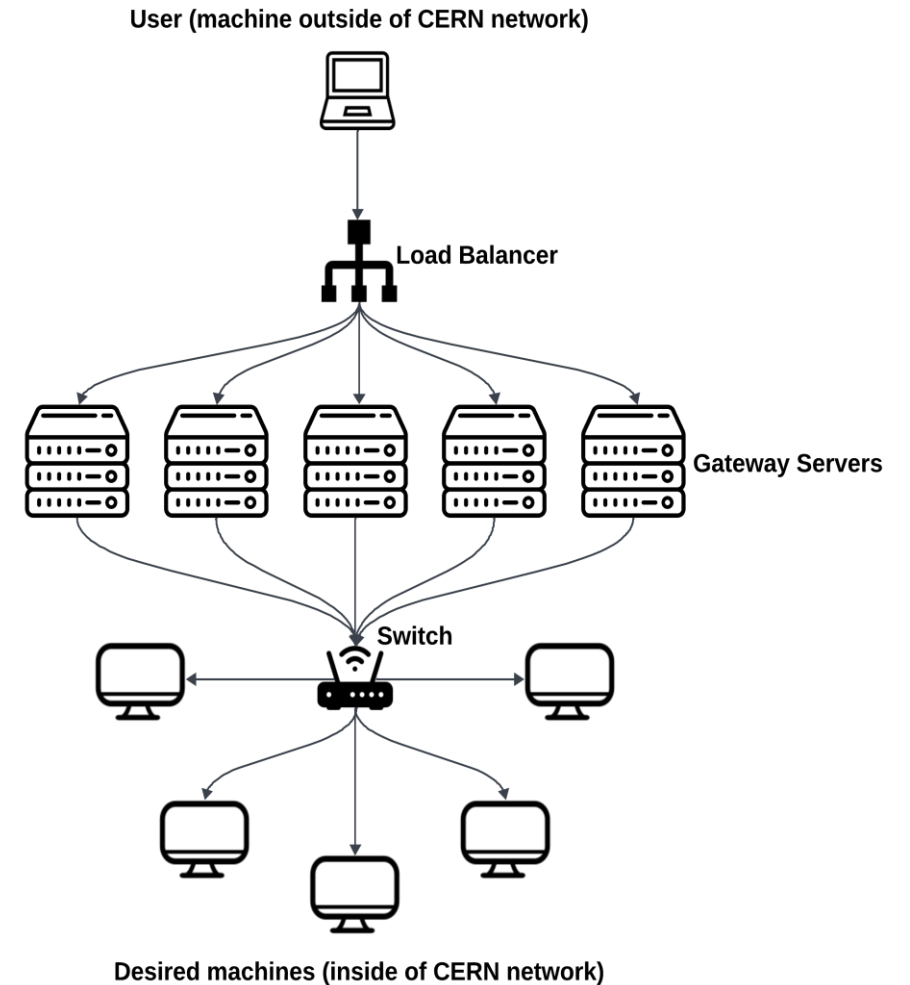
Allowing users to work effectively from outside and inside the CERN network, providing:

- Self-service
- Granularity
- Using existing Windows stack
- Security
- Maintenance
- Flexibility
- User-friendliness

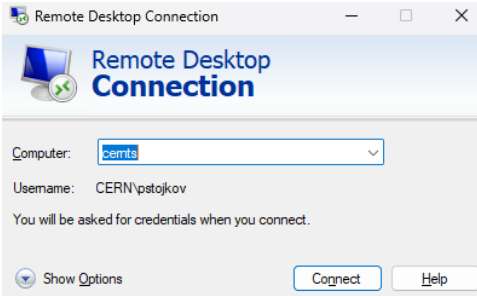


The Solution

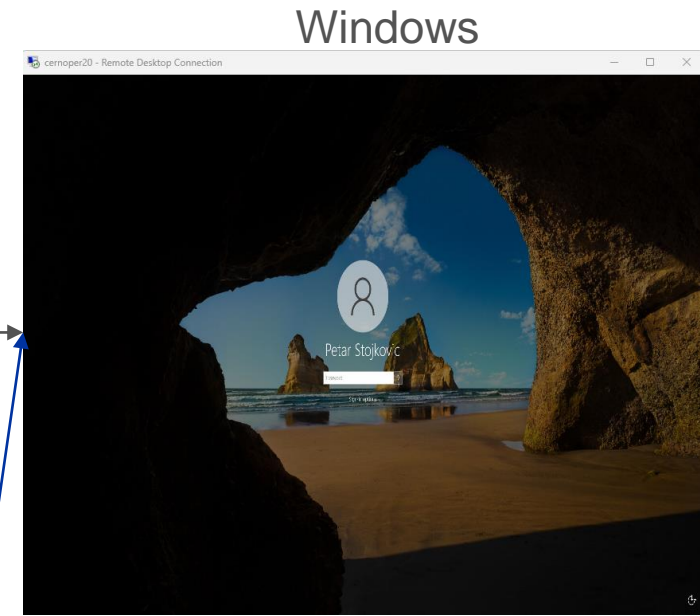
- A system enabling users to access their devices from outside CERN
- Configuration management
 - Self-service
 - Granularity
 - Security
 - Flexibility
 - Using existing Windows stack
- User-Friendly UI ————— Use- friendliness
- Data Cleaner ————— Maintenance
- Maintenance tools ————— Maintenance
- Session management ————— User-friendliness



RDP to Windows and Linux



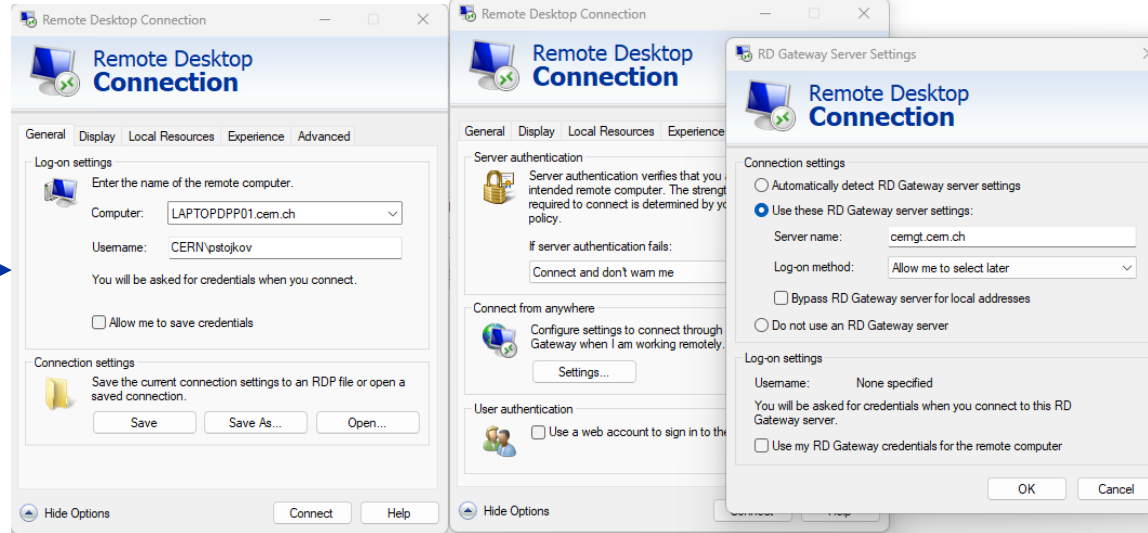
Remote to Terminal Server



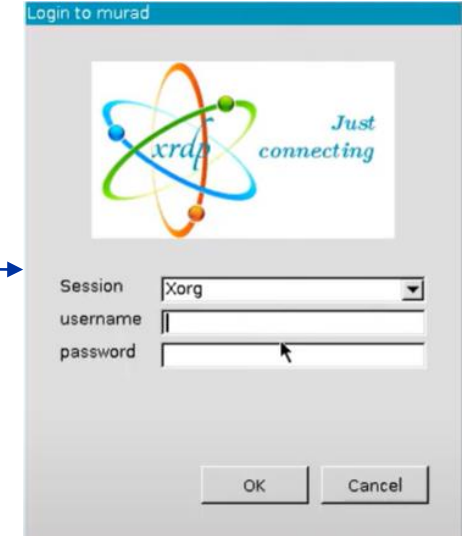
Remote Desktop Gateway

LAPITCA28R21.rdp

LAPTOPDPP01.rdp



Linux



Remote Desktop Service

CERN Accelerating science

Signed in as: pstojkov Sign out Directory

CERN Remote Desktop Service

Welcome to CERN Remote Desktop Service

If you're using this website for the first time, please read the instructions by clicking the help button on each page.

Help

Remote Desktop Gateway

Enable Remote Desktop Access to your devices from outside CERN.

Remote Desktop Gateway

Log Me Off

Disconnect your user sessions from Remote Desktop Terminal Services clusters.

Log Me Off

Log User Off

For Administrators. Disconnect users from Remote Desktop Terminal Services clusters you manage.

Log Users Off

Remote Desktop Debugger

For Administrators. Debug and verify Remote Desktop Terminal Services configurations.

Remote Desktop Debugger

Primary use cases

- **Remote Desktop Gateway** – Device configuration and user management
- Terminal Servers session management

Administrator use case

- Managing all configurations and accesses
- Terminal Servers session management of all users
- Debug tools and scripts

Key points: optimization, permissions, security, and convenience

Remote Desktop Service

CERN Accelerating science

Signed in as: pstojkov | Sign out | Directory

CERN Remote Desktop Service

Welcome to CERN Remote Desktop Service

If you're using this website for the first time, please read the instructions by clicking the help button on each page.

Welcome to the CERN Remote Desktop Service

Help

- Remote Desktop Gateway**
Enable Remote Desktop Access to your devices from outside CERN.
Remote Desktop Gateway
- Log Me Off**
Disconnect your user sessions from Remote Desktop Terminal Services clusters.
Log Me Off
- Log User Off**
For Administrators. Disconnect users from Remote Desktop Terminal Services clusters you manage.
Log Users Off
- Remote Desktop Debugger**
For Administrators. Debug and verify Remote Desktop Terminal Services configurations.
Remote Desktop Debugger

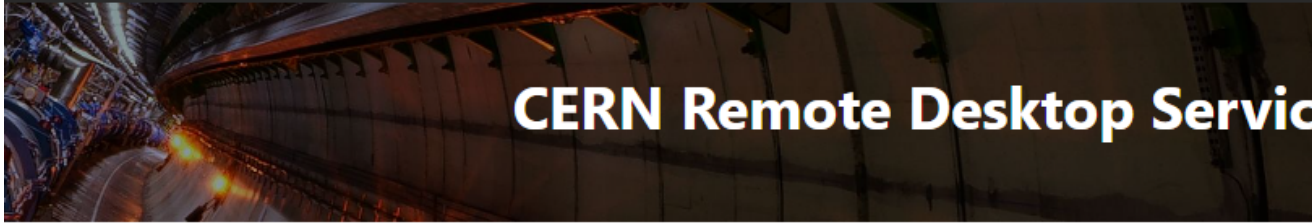
Primary use cases

- **Remote Desktop Gateway** – Device configuration and user management
- Terminal Servers session management

Administrator use case

- Managing all configurations and accesses
- Terminal Servers session management of all users
- Debug tools and scripts

Key points: optimization, permissions, security, and convenience



CERN Remote Desktop Service

Welcome to CERN Remote Desktop Service ✕
If you're using this website for the first time, please read the instructions by clicking the help button on each page.

Welcome to the CERN Remote Desktop Service

Help

Remote Desktop Gateway

Enable Remote Desktop Access to your devices from outside CERN.

Remote Desktop Gateway

Log Me Off

Disconnect your user sessions from Remote Desktop Terminal Services clusters.

Log Me Off

Log User Off

For Administrators. Disconnect users from Remote Desktop Terminal Services clusters you manage.

Log Users Off

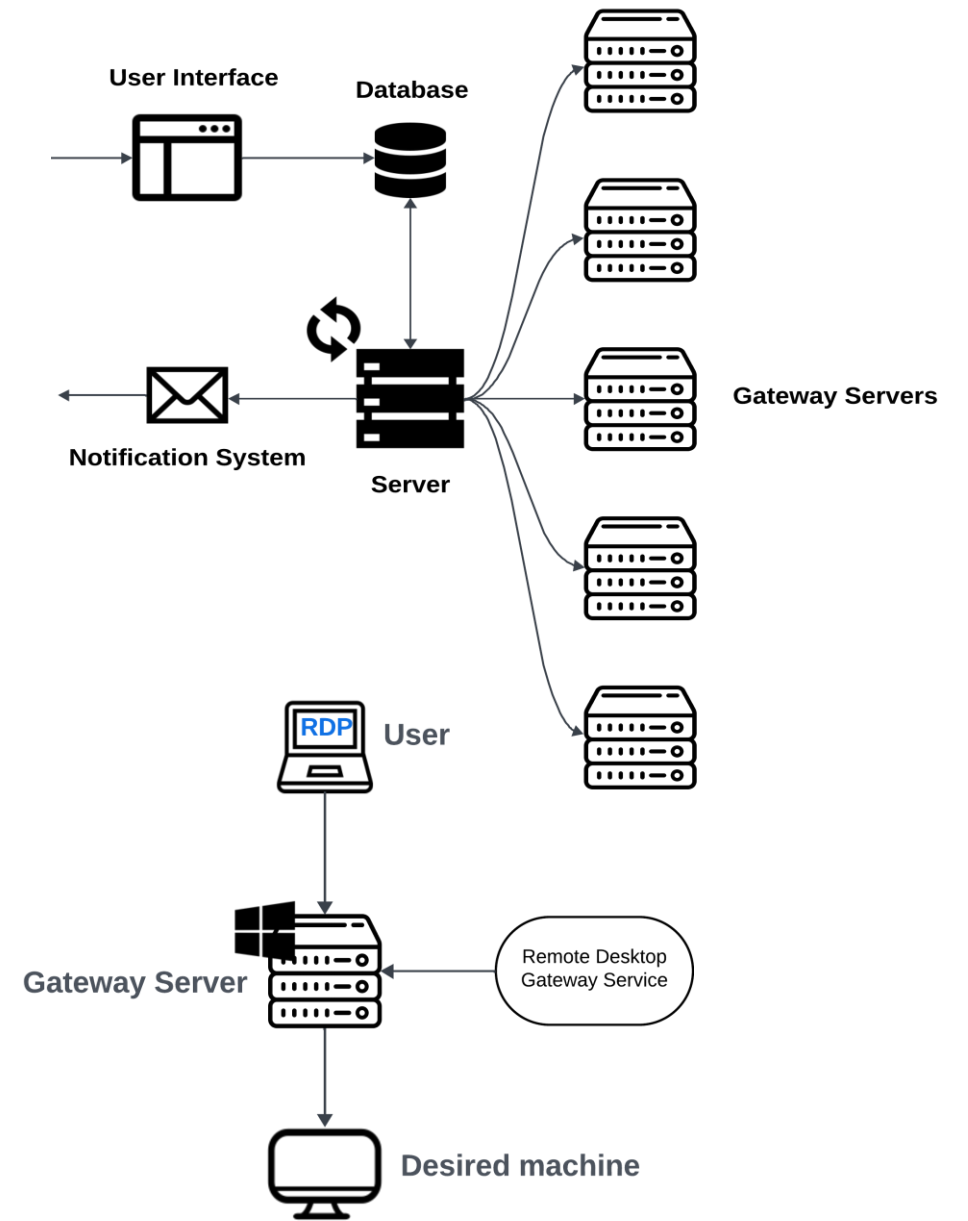
Remote Desktop Debugger

For Administrators. Debug and verify Remote Desktop Terminal Services configurations.

Remote Desktop Debugger

Remote Desktop Gateway

- Manage access for users' devices
- Synchronize accesses
- Notification system: Email users with status
- Gateway Server stack:
 - Windows server + Remote Desktop Gateway role
 - Local Groups
 - Remote Access Policies
- Clients' device stack:
 - Remote Desktop Users group



The Simple Steps to Remote Access

The screenshot shows a web interface titled "Manage Remote Desktop access to your devices from outside CERN". It features a navigation bar with "Home" and "Help" buttons. The main content is divided into two panels. The left panel, "Your remote-enabled devices", contains a search bar, a "Configure device" button (circled in red), and a "Download RDP file" button. Below these are several device entries, each with a status icon (checkmark or question mark), a name, and a "Mark as Synchronized" button. The right panel, "Manage user access for a configured device", contains a text input field for "Enter device name..." and a "Manage users" button.

Home Manage Remote Desktop access to your devices from outside CERN Help

Your remote-enabled devices

Search **Configure device** Download RDP file

Devices

✓	CERNMECM01					
?	CERNMECM02	Mark as Synchronized				
?	CERNOPER20	Mark as Synchronized				
?	LAPTOPPPP01	Mark as Synchronized				
✓	PCADMINI5H017					
✓	PCADMINI7H68					
✓	PCPADMINI7H03					
?	TETRA-NMS-B58	Mark as Synchronized				

Manage user access for a configured device

Enter device name... Manage users

The Simple Steps to Remote Access

The screenshot displays a web application interface for managing remote desktop access. The main heading is "Manage Remote Desktop access to your devices from outside CERN". The interface is divided into two main sections:

- Your remote-enabled devices:** This section contains a search bar, a "Hide configure device" button, and a "Download RDP file" button. Below these is a text input field containing "laptopdpp01" and a "+ Add" button. A green notification bar states "Successfully added the device!". Below this is a list of devices with their names and status icons (checkmark or question mark). Each device has a "Mark as Synchronized" button and a set of action icons (edit, download, refresh, delete).
- Manage user access for a configured device:** This section contains a text input field for "Enter device name..." and a "Manage users" button.

A red oval highlights the "laptopdpp01" device name and the "+ Add" button in the "Your remote-enabled devices" section.

Device Name	Status	Actions
CERNMECM01	✓	[Edit] [Download] [Refresh] [Delete]
CERNMECM02	?	[Mark as Synchronized] [Edit] [Download] [Refresh] [Delete]
CERNOPER20	?	[Mark as Synchronized] [Edit] [Download] [Refresh] [Delete]
PCADMINI5H017	✓	[Edit] [Download] [Refresh] [Delete]
PCADMINI7H68	✓	[Edit] [Download] [Refresh] [Delete]
PCADMINI7H03	✓	[Edit] [Download] [Refresh] [Delete]
TETRA-NMS-B58	?	[Mark as Synchronized] [Edit] [Download] [Refresh] [Delete]

The Simple Steps to Remote Access

The screenshot shows a web interface titled "Manage Remote Desktop access to your devices from outside CERN". It features a navigation bar with "Home" and "Help" buttons. The main content is divided into two panels. The left panel, "Your remote-enabled devices", contains a search bar, "Configure device", and "Download RDP file" buttons. Below is a list of devices with status icons and action buttons. The right panel, "Manage user access for a configured device", has an input field for "Enter device name..." and a "Manage users" button. A red circle highlights the "Download RDP file" icon for the device LAPTOPDPP01.

Home Help

Manage Remote Desktop access to your devices from outside CERN

Your remote-enabled devices

Search Configure device Download RDP file

Devices

✓	CERNMECM01					
?	CERNMECM02	Mark as Synchronized				
?	CERNOPER20	Mark as Synchronized				
✗	LAPTOPDPP01					
✓	PCADMINI5H017					
✓	PCADMINI7H68					
✓	PCPADMINI7H03					
?	TETRA-NMS-B58	Mark as Synchronized				

Manage user access for a configured device

Enter device name... Manage users

The Simple Steps to Remote Access

Home Manage Remote Desktop access to your devices from outside CERN Help

Your remote-enabled devices

Search Hide configure device Download RDP file

laptopdpp01 Add

Devices

Device	Status	Actions
CERNMECM01	✓	Share, Download, Refresh, Delete
CERNMECM02	? Mark as Synchronized	Share, Download, Refresh, Delete
CERNOPER20	? Mark as Synchronized	Share, Download, Refresh, Delete
LAPTOPDPP01	✓	Share, Download, Refresh, Delete
PCADMINI5H017	✓	Share, Download, Refresh, Delete
PCADMINI7H68	✓	Share, Download, Refresh, Delete
PCADMINI7H03	✓	Share, Download, Refresh, Delete
TETRA-NMS-B58	? Mark as Synchronized	Share, Download, Refresh, Delete

Manage user access for a configured device

laptopdpp01 X Manage users

Device: LAPTOPDPP01 + Add new user Download Delete

List of users with access for a device

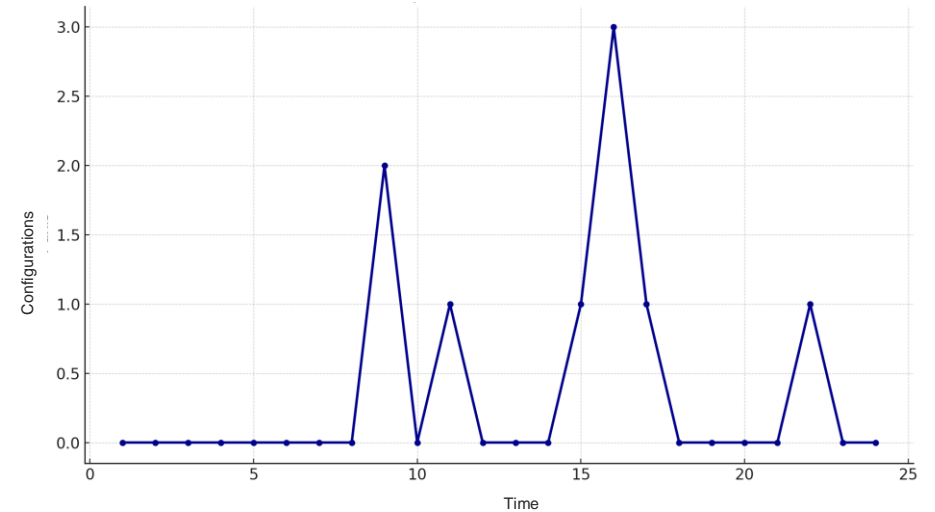
User	Actions
admpetar	Lock, Refresh, Delete
ricardom	Lock, Refresh, Delete
pstojkov	Lock, Refresh, Delete

Remote Desktop Gateway in Numbers

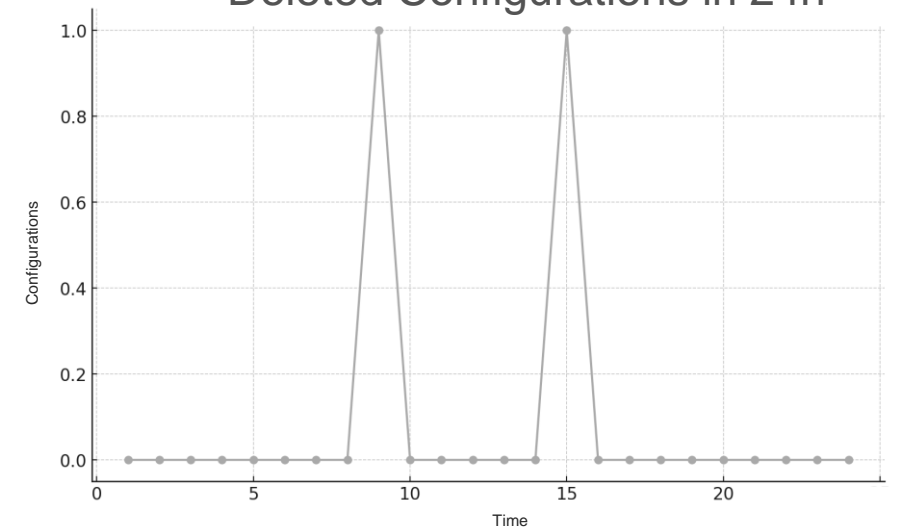
- Over **500+** daily users
- In total **4 600+** unique users
- Configured RDP **6 400+** machines
 - Windows machines (+ Linux machines)
- In total, more than **10 000+** configurations
- **5** Gateway servers

- **Daily** number of unique users: **501**
- **Daily** number of connections: **2 492**
- **Monthly** number of unique users: **1642**
- **Monthly** number of connections: **55 445**

New Configurations in 24h

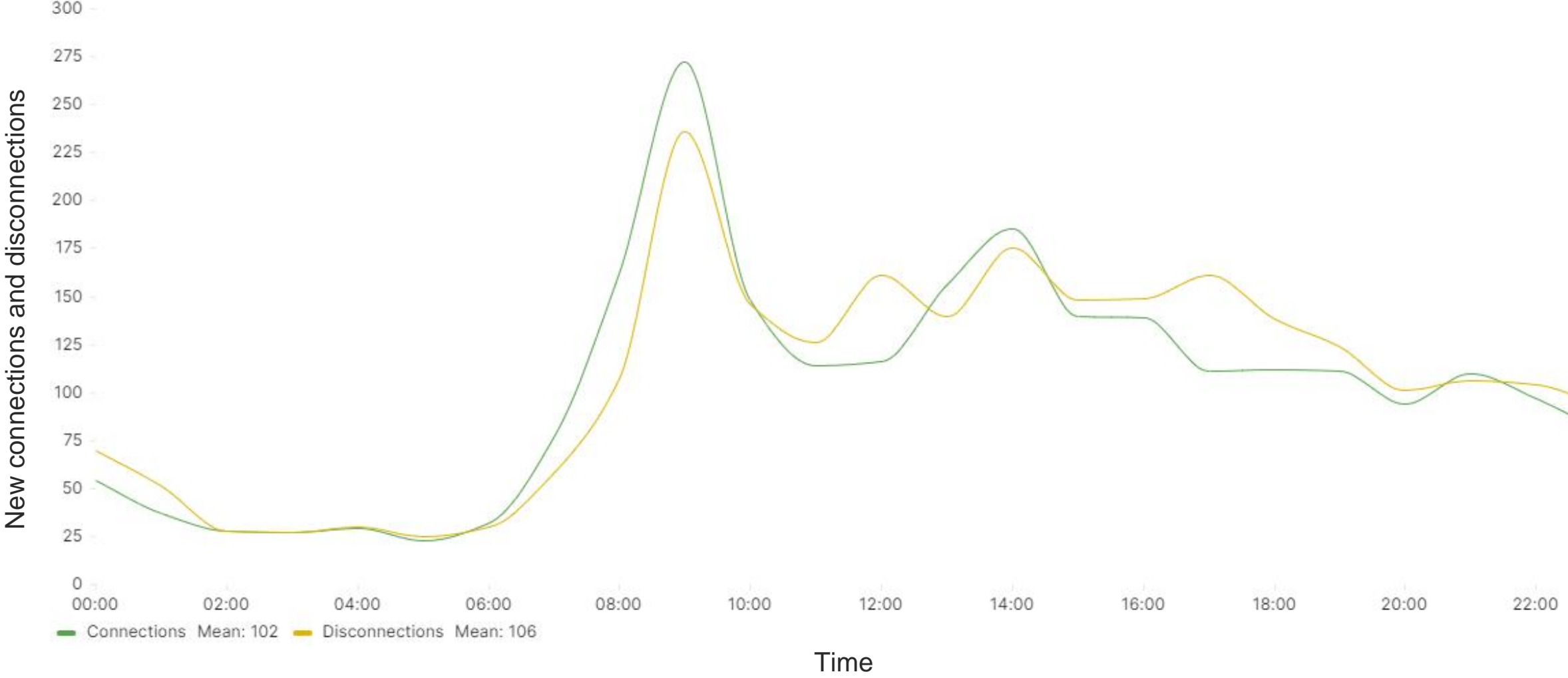


Deleted Configurations in 24h

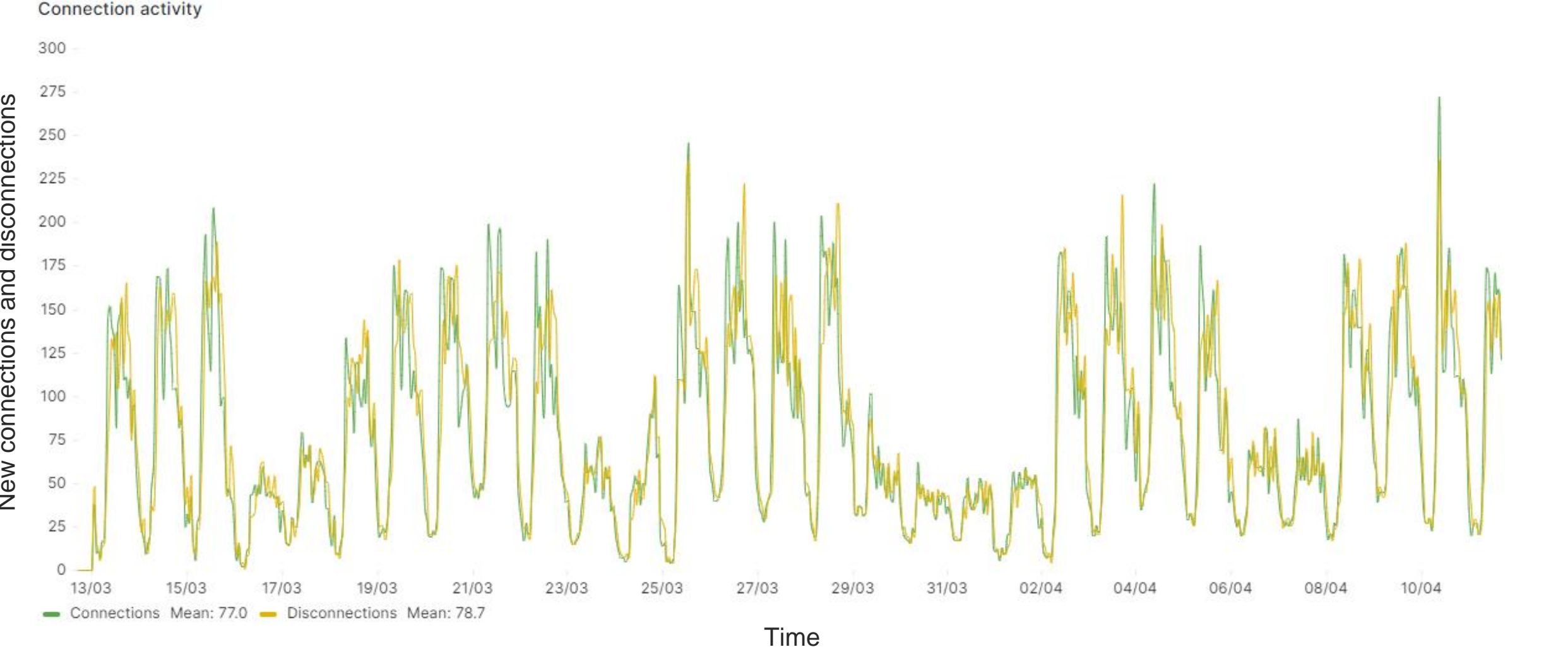


Established new (dis)connections in 24h

Connection activity

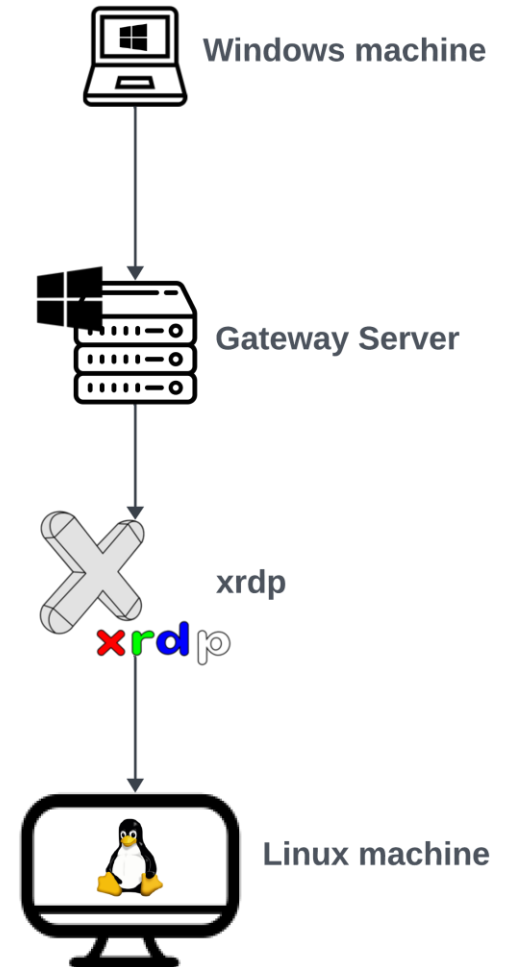


Established new (dis)connections in 30 days



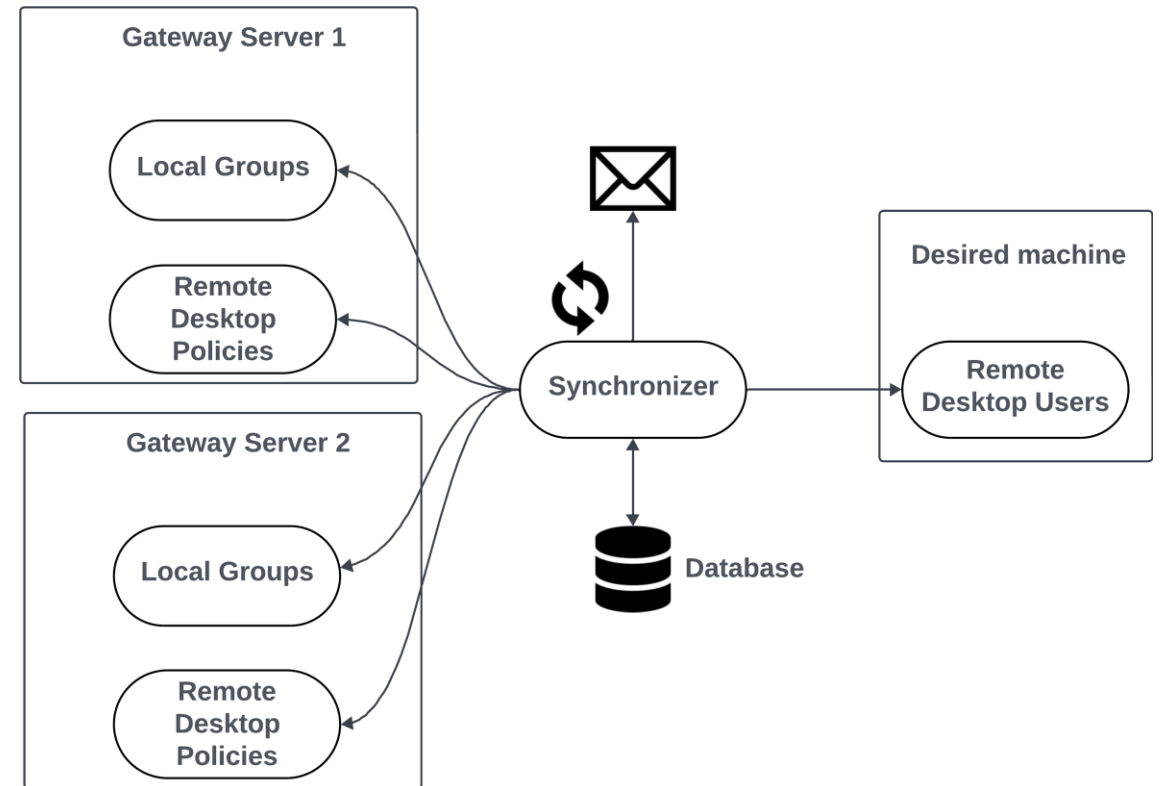
It also works for **Linux**

- Configure Linux machine on **Remote Desktop Gateway Website**
- On a Linux machine, configure **xrdp**
- Use the **RDP** file downloaded from **Remote Desktop Gateway Website**



The Muscle behind: The Synchronizer

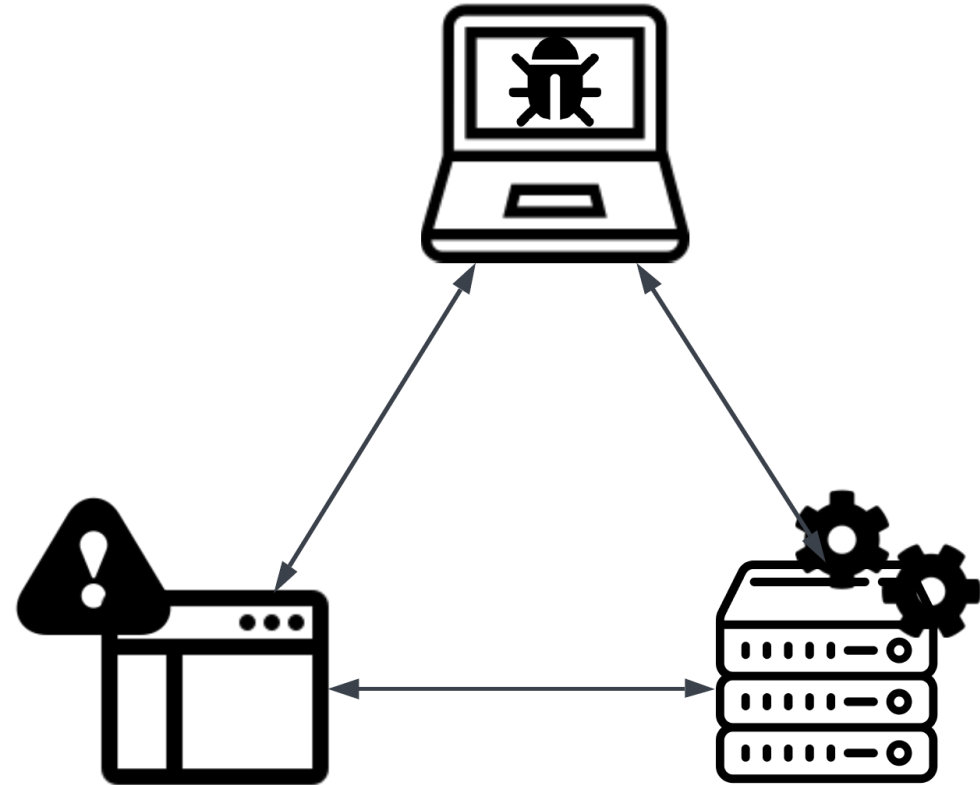
- Synchronization of 5 Gateway Servers in parallel
 - Makes sure that all gateways are synchronized
 - Manage Local Groups
 - Manage Remote Access Policies
- Manage Remote Desktop Users group (Windows client)
- Manage configuration updates in the database
- Logs operations
- Notify the user when device is configured
- Handles various scenarios and exceptions

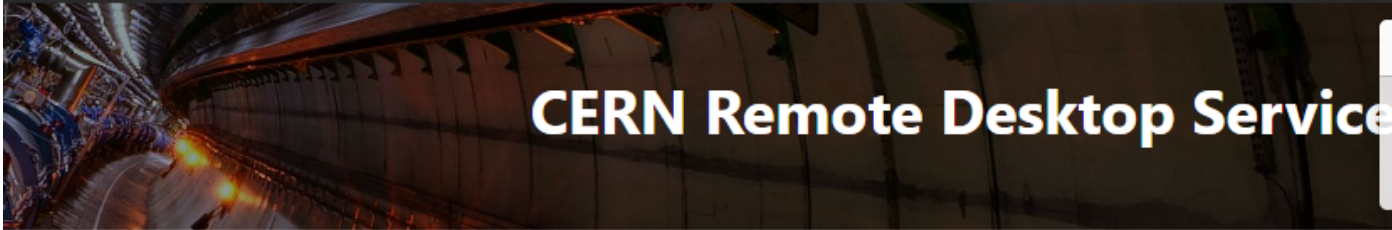


- Gateway Server 3
- Gateway Server 4
- Gateway Server 5

Obstacles and hic-ups during development

- Build around legacy technology:
 - Slow policy handling with limited space
 - Performance bottleneck
 - Data corruption
- Failed synchronizations
- Permissions





CERN Remote Desktop Service

Welcome to CERN Remote Desktop Service ✕
If you're using this website for the first time, please read the instructions by clicking the help button on each page.

Welcome to the CERN Remote Desktop Service

Help

Remote Desktop Gateway
Enable Remote Desktop Access to your devices from outside CERN.

Remote Desktop Gateway

Log Me Off
Disconnect your user sessions from Remote Desktop Terminal Services clusters.

Log Me Off

Log User Off
For Administrators. Disconnect users from Remote Desktop Terminal Services clusters you manage.

Log Users Off

Remote Desktop Debugger
For Administrators. Debug and verify Remote Desktop Terminal Services configurations.

Remote Desktop Debugger

Session Management

- Users can view and terminate their active sessions **in Terminal Servers**
 - Managing all Terminal Server cluster sessions
 - Decrease the need for support (e.g. session freezing)
- For administrators, the ability to manage all **users'** sessions

Home Help

Disconnect your user sessions from Remote Desktop Terminal Services clusters

Search cluster names Search machine names Current view: Public Clusters Only Show All Clusters

Cluster Name	Machine Name	Action
cernts	cernts1601	Log Off



CERN Remote Desktop Service

Welcome to CERN Remote Desktop Service ✕
If you're using this website for the first time, please read the instructions by clicking the help button on each page.

Welcome to the CERN Remote Desktop Service

Help

Remote Desktop Gateway
Enable Remote Desktop Access to your devices from outside CERN.

Remote Desktop Gateway

Log Me Off
Disconnect your user sessions from Remote Desktop Terminal Services clusters.

Log Me Off

Log User Off
For Administrators. Disconnect users from Remote Desktop Terminal Services clusters you manage.

Log Users Off

Remote Desktop Debugger
For Administrators. Debug and verify Remote Desktop Terminal Services configurations.

Remote Desktop Debugger

Debugger

- Identifying and resolving issues
- No need for in-depth technical knowledge of the system
- Easy system maintenance
- Synchronization status check
- Easy pick up by new supporters

Home Help

Debug User Configurations on Gateway Servers and Database

pstojkov Fetch User Info

Database: RAP Content

Enabled: Yes

Resource Group Name: LG-pstojkov

Synchronized: Yes

To delete: No

Unsynchronized Gateways: None

Gateway Servers Local Groups Content

cerngt05

- cernmecm01
- cernmecm02
- cernoper20
- guarumo
- LAPTOPDPP01
- padmini5h017
- padmini7h68
- pcpadmini7h03
- pstojkov
- tetra-nms-b58

cerngt06

- cernmecm01
- cernmecm02

Database: RAP Resources Content

CERNMECM01 ^

Resource Owner: CERN\WINDOWS-SERVERS-CORE

Access: Yes

Synchronized: Yes

Invalid: No

Incomplete sync: No

To delete: No

Unsynchronized Gateways: None

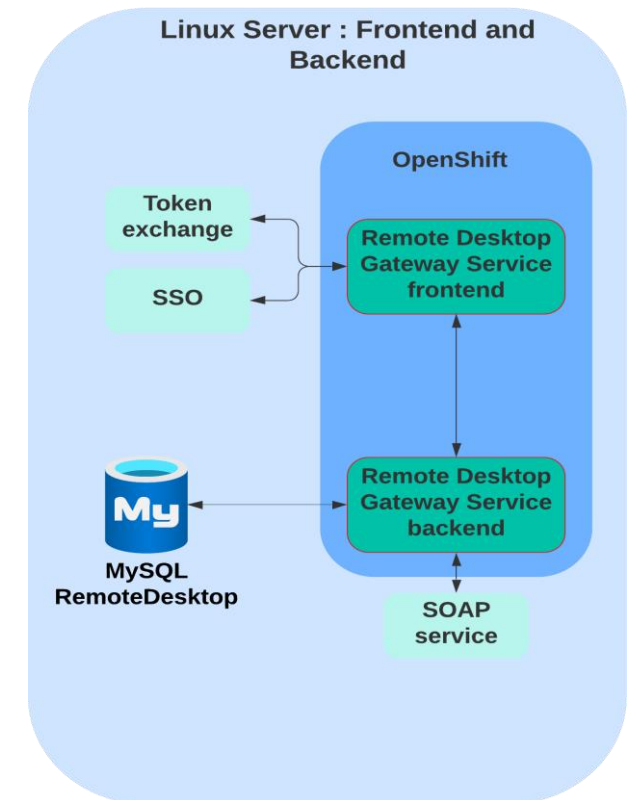
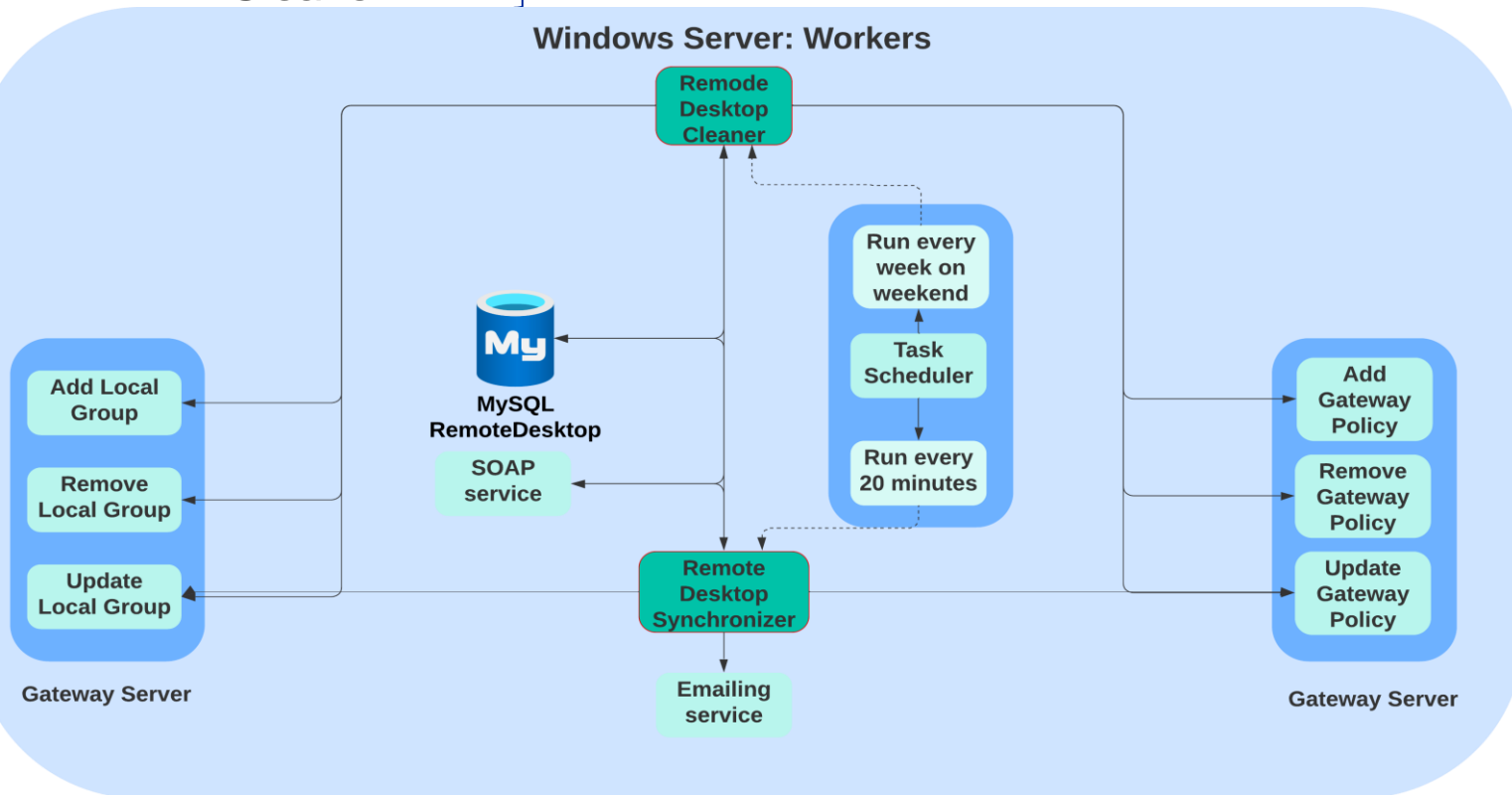
CERNMECM02 v

CERNOPER20 v

Architecture

Remote Desktop Service

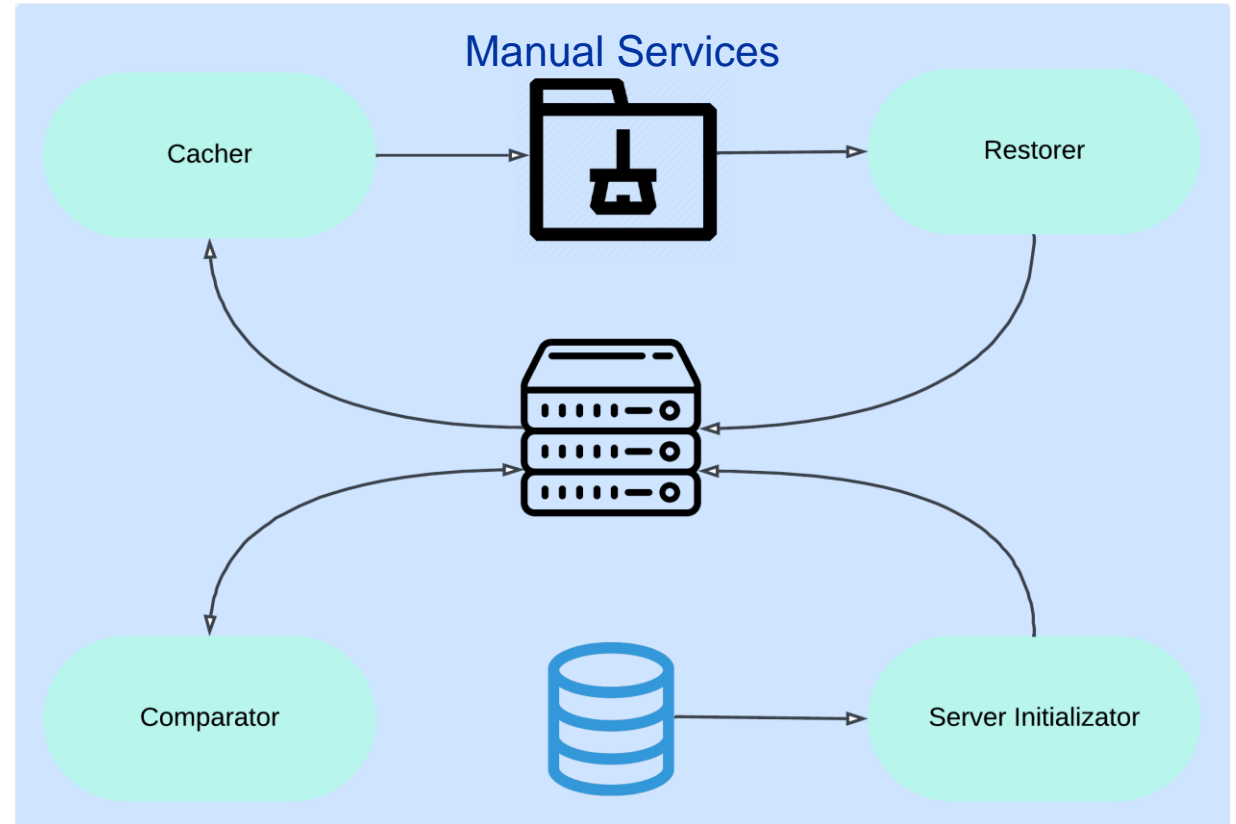
- Frontend
 - Backend
 - Synchronizer
 - Cleaner
- Deployed on Linux server with OKD and Docker (image, repository and config triggers)
- Deployed on Windows machine with Puppet and Task Scheduler



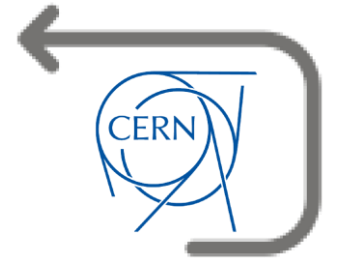
Architecture

Ad-hoc Services

- Run on demand
- Update gateway server with missing data
- Initialize new gateway servers
- Backup service configuration



Today we talked about how...



- Remote Desktop Gateway provides **self-service** and **granularity**
- It enables efficient work from outside and inside the CERN network
- It enables secure remoting to Windows and Linux machines
- User Interface provides easy usage with minimal training
- We bragged a bit about statistics and showed obstacles in development

Thank you for your attention

