A9X Scripting

Executive Summary

Often remotely located vessels face challenges with computer issues, and A9X Scripting is one of the tools that can allow remote intervention, allowing the computers to be accessed and returned to their normal operating capabilities.

A recent event on a ship required the office-based IT Support Team to try and connect to the ship using TeamViewer. After several attempts, no access to the network could be obtained locally nor via TeamViewer.

A9X Cyber Detective had previously been installed on the vessel's computers, and this allowed A9X Scripting to be used. An IT team can create and send scripts to any PC's on any of their vessels from the A9X Web Dashboard. The scripts can be written in PowerShell, Ruby or Python using an embedded version of Microsoft's VS Code IDE.

The Code Editor allowed simple command/script dispatching and reporting, making it quick and simple to trouble shoot the problem. The server time that was the problem source was detected, adjusted, all the machines were resynced and this solved the login issues. The ship's network was restored within a few hours using A9X Scripting service.

Background

The vessel's network consisted of several workstations running Windows 10 and a server (and DC) running Windows Server 2019. The server runs several services including A9X Cyber Detective, mail, RDP server and TeamViewer. For remote administration and support, the office connected to the server using TeamViewer and can then access the workstation PC's.

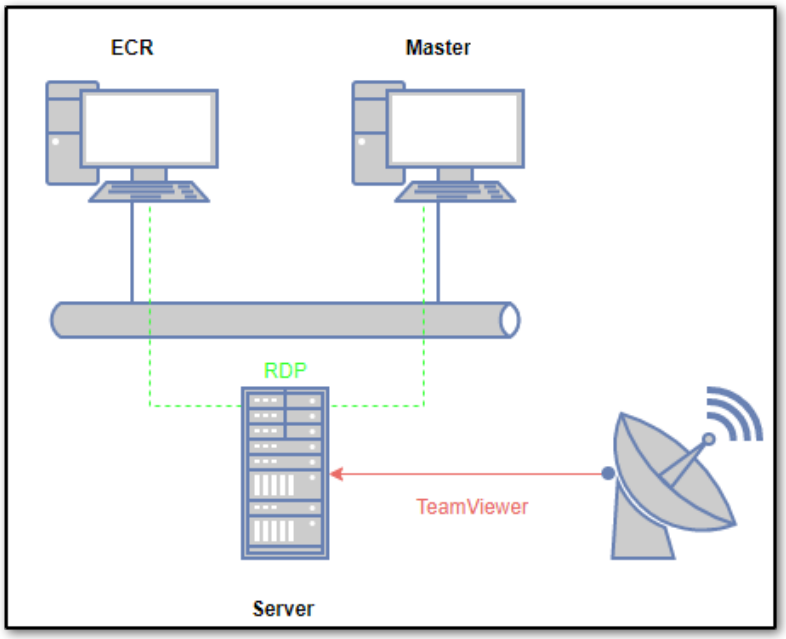

Figure 1 – Vessel IT Set-Up.

Trouble Strikes

The shipping companies IT Team received a support call from the vessel – the captain reported that they were having problems logging into their PC's. The team decided to remotely connect to the vessel using TeamViewer so they could see what was going on.

They connected to the server using TeamViewer, but when tried to login and saw an error message:

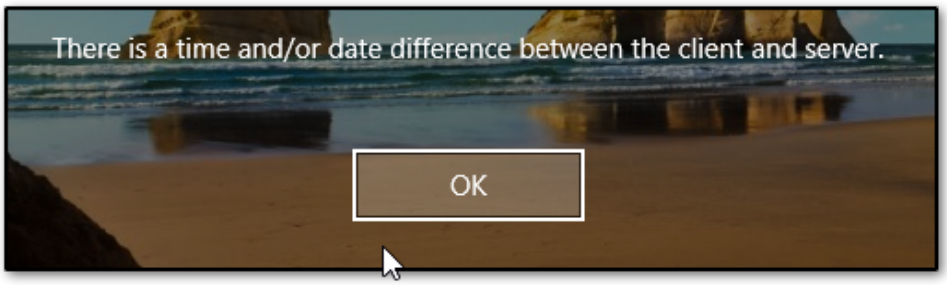

Figure 2 – Error Message: displayed on PC machines both locally and remotely.

This was the same error message being displayed from all the PC's both locally and remotely via TeamViewer. They were locked out of the server. This meant they were also unable to access any other PCs on the network as they were reached via RDP from the server machine. The business network was offline and there was no way to fix it. By this time, the captain reported that he had not been able to access his mail for several hours and the vessel was not due in port for serval days.

Utilizing A9X Scripting

With A9X Scripting, an IT Team can create and send scripts to any PC on any of their vessels from the A9X Dashboard, part of the service provided as part of A9X Cyber Detective. The scripts can be written in PowerShell, Ruby or Python using an embedded version of Microsoft's VS Code IDE. The scripting service is an optional module that's available for our Cyber Detective platform. Our support team quickly got to work to help the customer to resolve their problem.

We knew that our Cyber Detective service was still running normally and it could download, distribute and execute any commands we sent to it.

Problem Solving with A9X Scripting

We thought there could be either a problem with the Windows Time service (w32tm) not running, perhaps causing the server to fall back to the BIOS date. Or a problem with Windows not being able to sync the Microsoft NTP servers.

The first thing we did was to send this command to the server PC: **get-date.**

The response we got back was: **Tuesday, January 7, 2098 7:09:37 PM.**

The server's time was 70+ years in the future, in the year 2098. The workstations were failing to sync. with the server and still had the correct date.

Figure 3 - The Dashboard: shows commands being send to a remote PC, the status (Pending, Downloaded, Complete) and the result.

It was clear the time was corrupted on the server and time sync was not working. We tried several commands to fix the problem, from restarting the Windows Time service, forcing a time sync, getting the correct time from a different machine and then setting the date manually, overriding the bogus date/time.

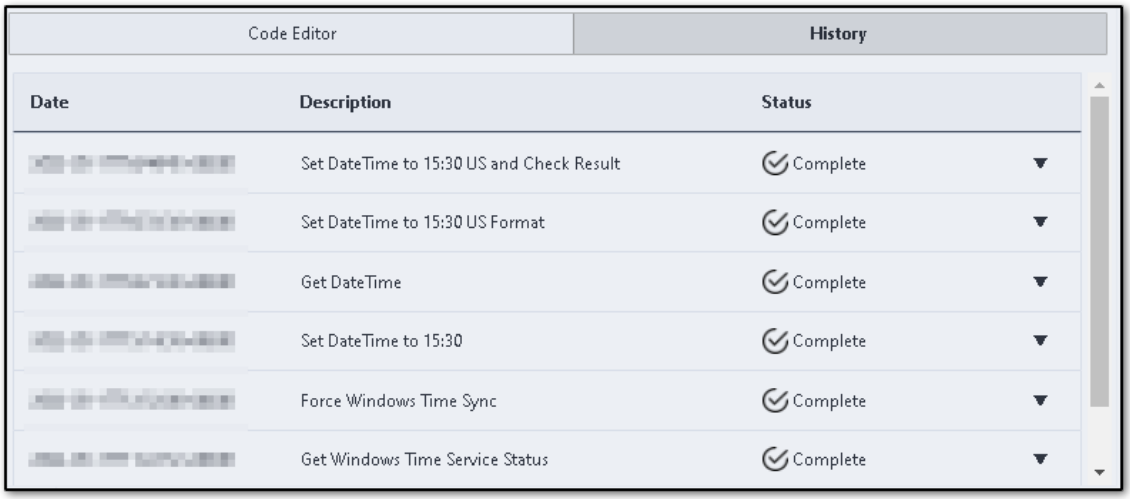

Figure 4 - The Code Editor: simple command/script dispatch and reporting made it quick and simple to trouble shoot the problem.

We fixed the server time, resynced all the machines and solved the login problem. The ship's network was restored within a few hours.

Find out more about our A9X Scripting Service at www.a9x-cybersecurity.com, or contact us on sales@a9x.com for a demonstration and FREE trial.

Chris Blunt
Director of Operations
A9X Cyber Security