Troubleshoot Standalone Umbrella Roaming Client Mass Deployment

Contents

Introduction

This document describes best practices for performing mass deployments of Umbrella Roaming Client and common issues to avoid.

Prerequisites

Requirements

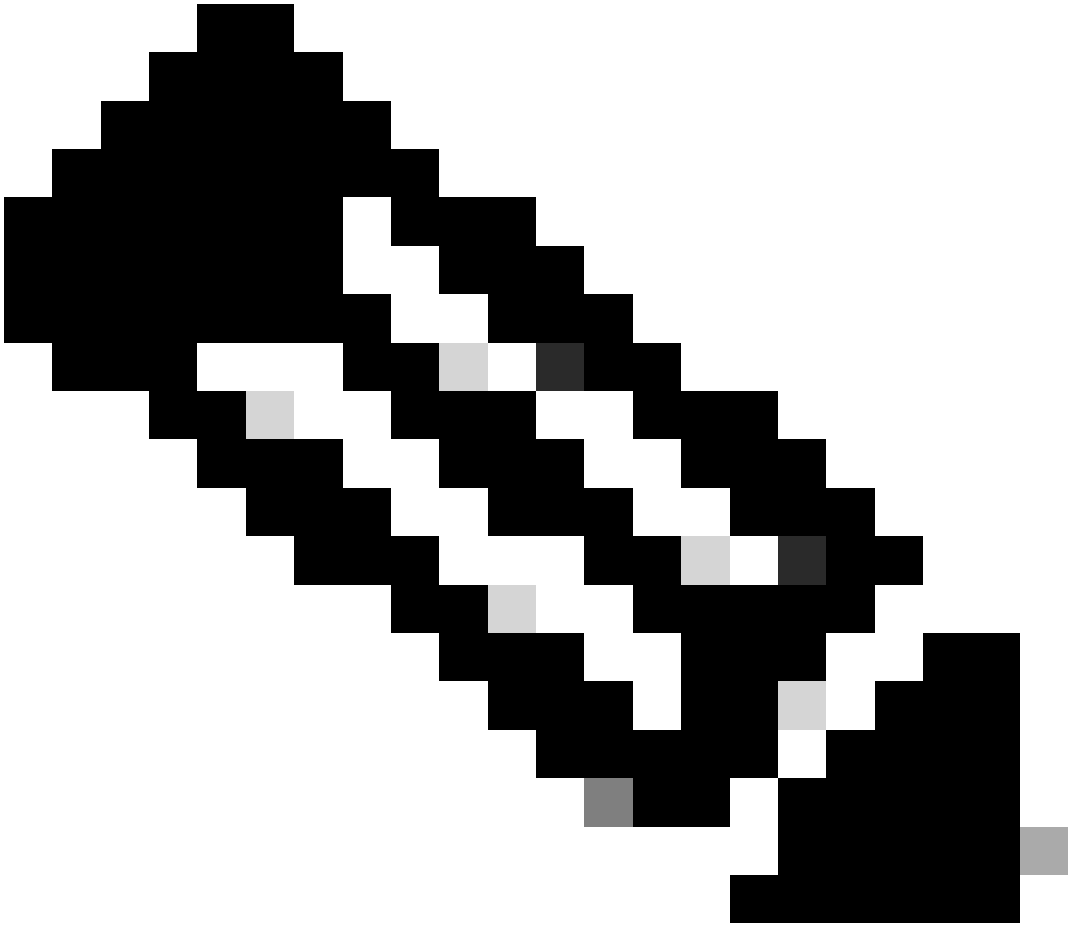
There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Roaming Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background



Note: This article is about the standalone Umbrella Roaming Client. For information on customizing mass deployment of the Cisco Secure Client (Formerly AnyConnect), see the Umbrella documentation for Windows and macOS.

In order to deploy the standalone Umbrella Roaming Client to a large number of machines at once, admins often choose to use a mass deployment program. Examples of this include Intune, System Center Configuration Manager (SCCM) or a Group Policy Object (GPO). Using such a system has a clear advantage with initial deployments but can present problems down the road if not properly handled. This article discusses Umbrella recommendations on the best practices for performing mass deployments and common issues to avoid.

Umbrella Upgrade Process

After initial installation, the Umbrella Roaming Client automatically checks for updates based on which release wave a company organization is using (either staging or one of Umbrella's production tracks). Once it sees that an update is available, it downloads the installer in the background. It then installs the new version and restarts the service automatically.

Mass Deployment Conflict

Umbrella Support has found that many customers leave their mass deployments on because they assume that the policy checks to see if any version of Umbrella is installed and can only install if none exists. However, the registry keys that are most commonly used to determine installation are actually specific to the build number. In other words, it does not check to see if Umbrella is installed, but for example, that Umbrella 3.0.17 is installed.

This results in this behavior:

1. The Umbrella Roaming client detects a new version is available and installs it.

2. Mass deployment tool detects that the registry key it is expecting to see for Umbrella is not present and triggers an install of the previously configured version.

3. The old version comes back online and checks for updates. It sees there is an update to be downloaded and installs it.

4. Process repeats to step 1.

Because of the competing update mechanisms, Umbrella constantly changes between the old version installed by the mass deployment tool and the new version being pulled down by Umbrella.

Issues

This can cause these issues:

- More time spent in unprotected state as Umbrella is frequently being restarted and initialized.
- Unexpected reboots or windows service failures (especially if the previous version being installed is 3.0.17, which has a known bug that causes forced reboot).
- System exposed to the bugs and security vulnerabilities that have already been fixed in the new version for approximately half of the time a machine is on and logged in.

Resolution

There are a few things you can do to address these issues:

1. Most importantly, it is best practice with Umbrella to only use mass deployment policies when you know there are new machines are being added to the network.

2. If you are going to run a mass deployment that installs if it does not detect an installation, be sure to use an installation metric that matches on any version of Umbrella instead of a specific version. To do this, please see Umbrella's KB article: How To: Verify Umbrella Roaming Client is installed on Windows via registry (any version number)

3. When setting up a new mass deployment policy, make sure you are getting the current build. You can see all of the available builds from Umbrella's release page. You can also subscribe to this list to get updates when a new version is being deployed.

Please note that this can include some builds that are not yet being pushed to your organization. To see what version your release track is giving you, download Roaming Client installer from your Umbrella dashboard.

Example Log Entries

See excerpts from log files here illustrating the flapping back and forth between a newer version downloaded automatically from Umbrella and an older version being pushed out by a mass deployment system.

- Original installation is observed (Starting version).
  `2021-11-30 02:44:07 [4228] [INFO ] < 3> ***** Starting ERC Service version 3.0.17`
- New version is is detected and downloaded.
  `2021-11-30 05:03:38 [4228] [DEBUG] < 18> Downloading:https://disthost.umbrella.com/roaming/upgrade/win/production/RoamingClient_WIN_3.0.110`
- Computer gracefully shuts down all of its components and restarts the**service**(not the machine).
  `Upgrade executed! If successful, the service should restart shortly...`
- We see it come up on new version (in this case, 3.0.110).
  `2021-11-30 05:09:45 [1436] [INFO ] < 4> ***** Starting ERC Service version 3.0.110`
- We see a log indicating that dnscryptproxy was abruptly interrupted (this is because of restart).
  `2021-11-30 05:33:43 [2136] [INFO ] < 33> DnsCryptProxy IPv4: dnscryptproxy.exe with (pid 8752) did not exit gracefully (fail count 0); restarting...`
- The old version returns to the logs.
  `2021-11-30 05:33:57 [7248] [INFO ] < 4> ***** Starting ERC Service version 3.0.17`