



## Best Practices for Server Monitoring & Problem Resolution

Network monitoring is a critical IT function, as it allows you to proactively prevent problems rather than wait for breakdowns to occur. Key to network monitoring, is server monitoring and establishing proper incident resolution and response parameters. One of the benefits of outsourcing is the value you gain of an organization experienced in working with and rolling out the following approach.

### *Categorize Servers and Issues into Priority Levels*

All problems are not created equal, and a successful network monitoring and management system recognizes this. In order to take a systematic approach to monitoring and managing your IT system, a good starting point is to begin by categorizing your servers and potential problems into priority levels. These priority levels, in turn, will dictate the response that will occur when issues arise.

At Coyote Creek we like to use a “P1 through P4” categorization system. Here’s how it looks:

- **P1** - This designation is reserved for the most business-critical items and functions. When something goes wrong with a P1 it must be addressed immediately, regardless of the hour. Our network monitoring clients understand that if, for example, a P1 server goes down at 3:00 in the morning, we’ll be working on the solution by 3:10 – and giving them a call at that hour to make them aware of the issue.

Examples of items and issues that might be categorized as “P1” include:

- External/internal mail WINS site servers
- Application system failures
- Network failures
- Hardware failures on P1-designated servers
- A P1 issue that results in an engineer being unable to work on a critical build or bug fix
- **P2** - This designation is for things that are “almost” as critical as P1 functions, but that don’t necessarily require middle-of-the-night attention. If something goes wrong with a P2 item during normal business hours it is addressed immediately. But if the problem occurs on the weekend or late at night, the solution might wait until the start of the next business day.
- At Coyote Creek our response to our monitoring clients’ P2 issues is nearly the same as our response to P1 issues – with one important exception. Although we’ll start working on the solution immediately, our client will receive an email rather than a 3:00 am phone call about the issue.
- **P3** - P3 issues are standard, “run of the mill” issues, not emergencies. An example of a P3 issue is the need to create a new account for a user. The account needs to be created, but not necessarily right at this moment.
- **P4** - The P4 designation is for things that need to get done, but are not critical at all. These could be items that you want to keep track of, such as a maintenance project or a non-critical patch update. These are the type of things that you take care of when everything else is running smoothly.

### *Determine Acceptable Response and Resolution Times*

Once you’ve categorized things by priority level, the next step is to decide in advance how quickly you’ll commit to getting things fixed at each priority level. Here’s what we commit to for our network monitoring clients:

- **P1** – Response is immediate, with a 2-hour resolution time
- **P2** – Response is immediate during business hours, with a 4-hour resolution time. If the problem occurs outside of business hours we’ll start working on it right away, but won’t escalate communications until the next business day.

- **P3** - Response within 4 business hours, resolution within 3 business days.
- **P4** - By definition P4 issues have no pre-set response or resolution times.

Organizations that handle their network monitoring and management in-house may choose not to respond to P2 issues until the next business day. However, the person responsible for fixing the problem may choose to get a middle-of-the-night alert so that he or she can get to the office early the next morning to start working on a solution.

#### ***Establish Your Escalation Policies***

When an issue arises, who will be responsible for addressing it? Who should be notified about the issue, and how quickly will this notification take place? At what point in the timeline should the second-, third-, and fourth-level contacts be informed about the issue?

Having a pre-established escalation process in place eliminates subjective judgment calls. If a P1 server goes down at 2:00 am, for example, the responsible person knows they must start working on a solution and call the IT Manager within 5 minutes. No need to waste time agonizing about whether or not to place the early morning wake-up call – it's company policy.

Typical escalation policies for a P1 issue might state that the immediate response includes a phone call to the Manager and an email to everyone on the escalation chain. Then the Director is also called if the problem isn't resolved within 15 minutes, and the Executive is called if the problem isn't resolved 15 minutes after that.

#### ***Conclusion***

In addition to enabling you to proactively detect and resolve problems, server monitoring is also important for capacity planning, meeting service level agreements, tracking your network's growth, and more. A vital part of any network monitoring and management system is to have a plan in place regarding how issues will be handled.