2.0 Werkzeugwahl, Kennzeichnungen und sichere Anwendung

Ziel dieser Seite

Diese Seite erklärt, wie für eine konkrete Diagnosefrage das passende Werkzeug ausgewählt wird. Sie legt außerdem die Kennzeichnungen fest, die in diesem Kapitel vor den Befehlen verwendet werden.

Die wichtigste Grundregel lautet:

> Erst die Diagnosefrage formulieren, dann das Werkzeug auswählen und erst danach den Befehl ausführen.

Ein Werkzeug ist ein Messinstrument. Es ersetzt weder eine Hypothese noch die Bewertung des Ergebnisses.

---

1. Grundhaltung bei der Werkzeugwahl

Administratoren sollten nicht möglichst viele Befehle ausführen, sondern mit möglichst wenigen, gezielten Prüfungen die Fehlerdomäne eingrenzen.

Vor jedem Befehl werden deshalb fünf Fragen beantwortet:

1. Was möchte ich mit diesem Befehl feststellen?
2. Welches Ergebnis erwarte ich bei einem funktionierenden System?
3. Welches Ergebnis würde meine Hypothese widerlegen?
4. Kann der Befehl den Zustand des Systems verändern?
5. Welche Daten muss ich zusammen mit dem Ergebnis dokumentieren?

Ein Befehl ohne konkrete Diagnosefrage erzeugt häufig nur zusätzliche Informationen, aber noch keine Erkenntnis.

Beispiel

Ungeeignete Fragestellung:

> Ich führe erst einmal alle Netzwerkbefehle aus.

Geeignete Fragestellung:

>

> Ich möchte feststellen, über welches Interface und welches Gateway der Client das Ziel `192.0.2.25` erreichen würde.

Dazu wird zunächst die Routingentscheidung geprüft. Ein Paketmitschnitt oder ein Portscan wäre zu diesem Zeitpunkt normalerweise noch nicht erforderlich.

---

2. Bedeutung der Kennzeichnungen

Die folgenden Kennzeichnungen stehen in diesem Buch vor Befehlen. Sie gehören nicht zum Befehl und dürfen nicht mit eingegeben werden.

Kennzeichnung	Bedeutung	Typische Auswirkung
`[RO]`	Read-only beziehungsweise nur lesende Abfrage	Liest Status oder Konfiguration aus, ohne sie absichtlich zu verändern
`[TEST]`	Aktiver Diagnosetest	Sendet kontrollierte Anfragen oder Testpakete
`[PRIV]`	Erhöhte Rechte erforderlich	Benötigt Administrator-, Root- oder vergleichbare Rechte
`[FILE]`	Erzeugt oder exportiert eine Datei	Benötigt einen geeigneten und geschützten Ablageort
`[SENS]`	Möglicherweise sensible Ausgabe	Kann interne Adressen, Namen, Benutzer-, Zertifikats- oder Nutzdaten enthalten
`[LOAD]`	Erzeugt relevante Last oder Datenverkehr	Kann Bandbreite, CPU, Speicher oder einen Zielservice belasten
`[CHANGE]`	Verändert Zustand oder Konfiguration	Erfordert Prüfung, Dokumentation und normalerweise einen Rückfallplan
`[DISRUPT]`	Möglicherweise dienstunterbrechend	Darf nur mit geklärter Auswirkung und entsprechender Freigabe eingesetzt werden

Kennzeichnungen können kombiniert werden.

Beispiele:

```
[RO] ip address
```
