

Podem o seguimento alternativo I, o relatório e o conjunto de dados quarantined do dispositivo do Gerenciamento de segurança (S A)?

Índice

[Pergunta](#)

[Resposta](#)

Pergunta

Posso eu suportar o seguimento, o relatório e o conjunto de dados quarantined do dispositivo do Gerenciamento de segurança (S A)?

Resposta

O dispositivo do Gerenciamento do Cisco Security (S A) permite que um administrador copie os conjunto de dados ativos (seguindo, relatando e base de dados ISQ) da “fonte” S à um “alvo” S A através do **comando backupconfig** no CLI.

O processo de backup é executado em duas fases:

Fase 1

Os começos do processo de backup com transferência de dados entre a fonte e os dispositivos do alvo. Durante transferência de dados, os serviços no dispositivo da fonte permanecem sendo executado, conseqüentemente o levantamento de dados pode ainda continuar. Os serviços são fechados embora no dispositivo do alvo. Uma vez que transferência de dados está completa da fonte visar o dispositivo, a fase 2 começa.

Fase 2

Quando a fase 2 começa, os serviços no dispositivo da fonte estão fechados. Todas as diferenças que recolherem durante transferência de dados entre a fonte e o dispositivo do alvo desde que a parada programada inicial é copiada ao dispositivo do alvo e ao serviço são trazidas o apoio para a fonte e o alvo. Isto permite o uptime máximo no dispositivo da fonte e a nenhuma perda de dados para um ou outro dispositivo.

Há dois tipos de backup agendado que você pode executar no S A:

Backup periódicos: Os backup periódicos consistem nos backup contínuos que podem ser programados por um horário pré-determinado, ou para um único backup que ocorra em um horário pré-determinado.

Backup imediatos: Os backup imediatos ocorrem imediatamente quando o usuário inicia o comando backupconfig no CLI.

Adicionalmente, você pode ver ou cancelar backup programados e em curso, verificar o estado de um backup, ou verificar se um backup pode ser programado em uma máquina remota.