

4. ALog ConVerter で使用するポートが知りたい

ALog ConVerter で使用するポートとその方向は以下の通りです。

Source	Destination	ポート番号(Destination)	用途
--------	-------------	--------------------	----

◆for Windows (エージェントレス方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (イベントログの収集/各種監査設定)
		TCP135、TCP 動的ポート	RPC (イベントログの収集/各種監査設定)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要

◆for Windows (エージェント方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (エージェントの設置/動作指令/削除)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要
対象サーバ	⇒マネージャーサーバ	TCP445	SMB (イベントログの転送)

◆for NetApp (7-mode または vFiler)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (イベントログの収集)
		TCP514	rsh (イベントログの強制ローテート/監査設定など)
		TCP22	ssh (監査設定など)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要
対象サーバ	⇒マネージャーサーバ	TCP1022 (※1)	rsh (イベントログの強制ローテート/監査設定など)

(※1) 1022 が使用中の場合、514 - 1021 の範囲にある未使用ポートが使われる。

(※) rsh を使用する場合、双方向のポート解放が必要。ssh を使用する場合、対象サーバ→マネージャーサーバの向きのポート解放は不要。

◆for NetApp (Cluster-Mode)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (イベントログの収集)
		TCP22	ssh (監査設定など)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要

◆for EMC

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (イベントログの収集)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要

◆for Isilon

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (監査ログの収集)
		TCP22	ssh (監査ログの収集/SID 情報収集)
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要

◆for SQL Server (エージェントレス方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (トレースログの収集)
		TCP1433	対象 SQL Server へのアクセス ※既定のインスタンスの場合
		UDP1434、TCP 動的ポート	対象 SQL Server へのアクセス ※名前付きインスタンスの場合

◆for SQL Server (エージェント方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (エージェントの設置/動作指令/削除)
		TCP1433	対象 SQL Server へのアクセス ※既定のインスタンスの場合
		UDP1434、TCP 動的ポート	対象 SQL Server へのアクセス ※名前付きインスタンスの場合
対象サーバ	⇒マネージャーサーバ	TCP445	SMB (トレースログの転送)

◆for Oracle (Windows-エージェントレス方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (イベントログの収集/トレースログ(XML)の収集)
		TCP135, TCP 動的ポート	RPC (イベントログの収集/各種監査設定)
		TCP1521	対象 Oracle Database へのアクセス

◆for Oracle (Windows-エージェント方式)

マネージャーサーバ	⇒対象サーバ	TCP445	SMB (エージェントの設置/動作指令/削除)
		TCP1521	対象 Oracle Database へのアクセス
対象サーバ	⇒マネージャーサーバ	TCP445	SMB (イベントログ/トレースログ(XML)の転送)

◆for Oracle (Linux-エージェントレス方式)

マネージャーサーバ	⇒対象サーバ	TCP1521	対象 Oracle Database へのアクセス
		TCP21、TCP 動的ポート	FTP (トレースログ収集) ※パッシブモード ※SFTPとの択一
		TCP22	SFTP (トレースログ収集) ※FTPとの択一

◆for Linux

マネージャーサーバ	⇒対象サーバ	TCP22	ssh(監査設定、audit ログや syslog の収集) ※対象サーバ追加時にポート番号を指定可能
		ICMP エコー要求の受信許可	対象サーバ追加時 Ping チェック ※チェックを行なう場合のみ必要

◆Web コンソール

ブラウザ動作マシン	⇒マネージャーサーバ	TCP80	HTTP (Web コンソールへのアクセス) ※インストール時に任意値を指定可能
マネージャーサーバ	⇒マネージャーサーバ	TCP10041	内部 DB で使用